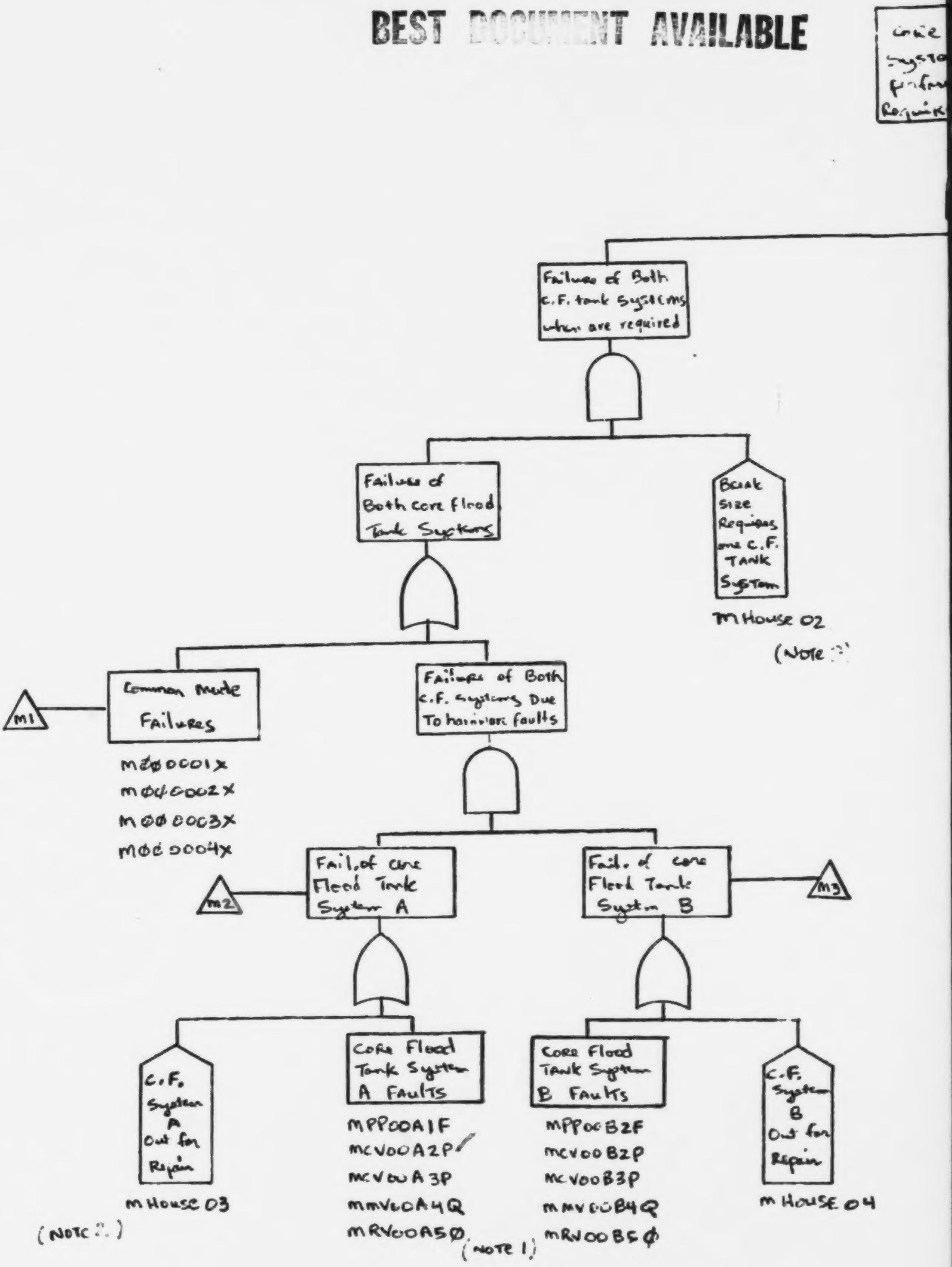
Table H.1 Core Flood System Fault Summary

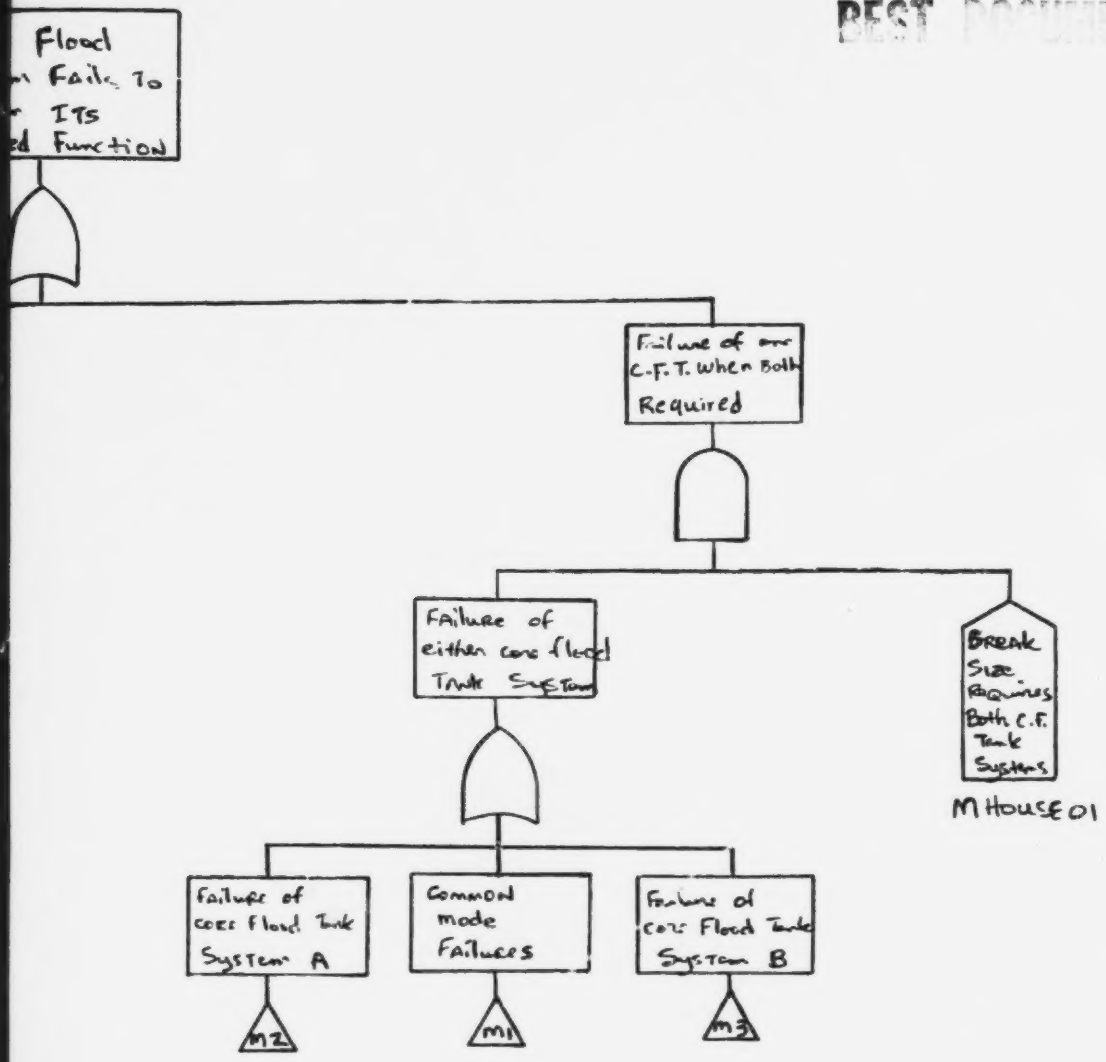
SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
M000001X	Insufficient BORON Concentration in Core Flood Tanks	Operator Error (Omission)
M000002X	Insufficient Water Volume in Core Flood Tanks	Operator Error (Omission)
M000003X	Insufficient Nitrogen Pressure in Core Flood Tanks	Operator Error (Omission)
MPP00A1F	Piping Between CFV-1 and RV	Rupture
MCV00A2P	Check Valve CFV-1	Does Not Open
MCV00A3P	Check Valve CFV-2	Does Not Open
MMV00A4Q	Motor Operated Valve CFV-5F	Does Not Remain Open (Plug)
MRV00A5Q	Relief Valve CFV-24F	Does Not Remain Closed
MPP00B1F	Piping Between CFV-3 and RV	Rupture
MCV00B2P	Check Valve CFV-3	Does Not Open
MCV00B3P	Check Valve CFV-4	Does Not Open
MMV00B4A	Motor Operated Valve CFV-6F	Does Not Remain Open (Plug)
MRV00B50	Relief Valve CFV-23F	Does Not Remain Closed
M000004X	Miscalibration of Level and Pressure Instrumentation	Operator Error (Commission)

BEST DOCUMENT AVAILABLE



Core
System
Perform
Require
Failure of Both
C.F. tank Systems
when are required
Failure of
Both core Flood
Tank Systems
Break
Size
Requires
one C.F.
TANK
System
M House 02
(NOTE 2)
M1
Common Mode
Failures
M000001X
M000002X
M000003X
M000004X
Failures of Both
C.F. Systems Due
To hardware faults
M2
Fail. of core
Flood Tank
System A
Fail. of core
Flood Tank
System B
M3
C.F.
System
A
Out for
Repair
M House 03
(NOTE 2)
Core Flood
Tank System
A Faults
MPP00A1F
MCV00A2P
MCV00A3P
MMV00A4Q
MRV00A50
(NOTE 1)
Core Flood
Tank System
B Faults
MPP00B2F
MCV00B2P
MCV00B3P
MMV00B4Q
MRV00B50
C.F.
System
B
Out for
Repair
M HOUSE 04

BEST DOCUMENT AVAILABLE


Flood
Fails To
ITS
Function
Failure of one C.F.T. When Both Required
Failure of either core flood Tank System
Break Size Requires Both C.F. Tank Systems
M HOUSE 01
Failure of core flood Tank System A
Common mode Failures
Failure of core Flood Tank System B
M2
M1
M3

NOTES:
1. Relief valve opening inadvertently would be immediately detected.
2. Only M House 01 or 02 will be on at one time. Similarly M House 03 or 04 will not be on concurrently. One system can be out for 1 hr for repair before going to hot shutdown.

Figure H.2 Simplified Fault Tree - Core Flood System (For Fault Summary see Table H.1)

H3 SYSTEM QUANTIFICATION

H.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The CFS is a double train system, but the success requirements depend on the size LOCA and operation of other systems (see Table H.2). For accidents where CFS is required, both trains are required to function, except in the case where the break occurs in one of the core flood lines downstream of the check valve; in this case the other core flood train is required to function. Thus, failure of either train will, in general, result in system failure. The system is entirely independent of other system interfaces, as no AC power or component cooling are required. Thus, the system unavailability is dependent only on check valves opening, and a small maintenance outage contribution.

H.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the CFS unavailability for required emergency operation. A modularized fault tree was constructed from the simplified fault tree to show CFS unavailability in terms of major gates, each gate consisting of collections of component failures or outages. Table H.2 shows the CFS success requirements, Table H.3 contains the top event definitions for the modularized fault tree, and Figure H.3 shows the modularized fault tree with the unavailability of each gate and the top event. Table H.4 shows the Boolean equation that represents the fault tree. Table H.5 , the quantification table, shows the quantification of each gate, and the attached notes explain the assumptions used in the quantification. Table H.6 summarizes the point estimates for each gate.

Table H.2 Core Flood System — Success Requirements

INITIATOR	TRAINS	NOTES
B_4	Not required	
B_3	Not required	
B_2	2/2 tanks	1
	0/2 tanks	2
	1/1 tanks	3
B_1	2/2 tanks	

NOTES:

1. 2/2 core flood tanks (CFT) are required if only 1/2 LPI trains are operable.
2. CFT are not required if both LPI trains are operable.
3. If the break occurs in the core flood line the remaining CFT and the associated LPI train (ore one HPI train) are required for success. This case was not analyzed.

Table H.3 Core Flood System — Top Events

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
CA	Failure of core flood tank A to deliver contents to reactor vessel at 600 psi reactor coolant pressure	1
CB	Failure of core flood tank B to deliver contents to reactor vessel at 600 psi reactor coolant pressure	1
CFS	Failure of either core flood tank to deliver contents to reactor vessel at 600 psi reactor coolant pressure.	2

NOTES: 1. This top event is defined as a convenience to facilitate the quantification of CFS

2. For the cases analyzed either both core flood tanks are required (B_1-LOCA and B_3-LOCA where one LPI-train is inoperable) or no core flood tanks are required (B_3-LOCA with both LPI-trains operating).

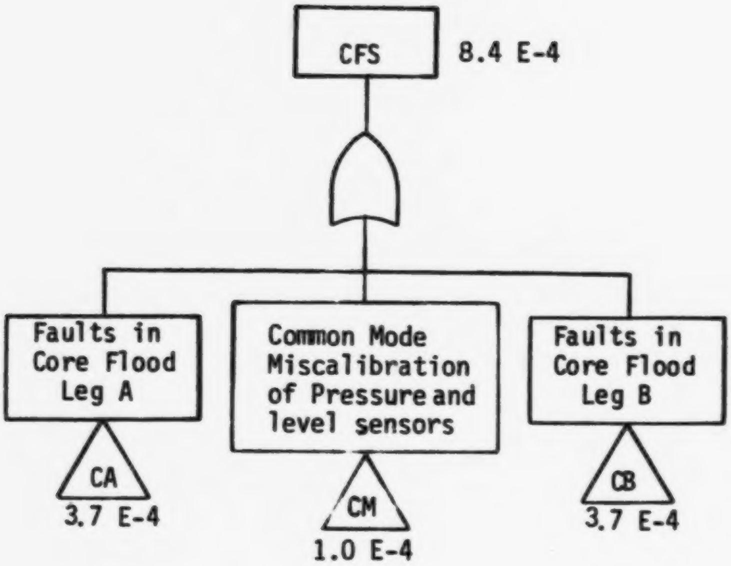

CFS
8.4 E-4
Faults in Core Flood Leg A
CA
3.7 E-4
Common Mode Miscalibration of Pressure and level sensors
CM
1.0 E-4
Faults in Core Flood Leg B
CB
3.7 E-4

Figure H.3 Modularized Fault Tree for Event "CFS"

Table H.4 Core Flood System

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT

CFS = CA + CB + CM

BEST DOCUMENT AVAILABLE

Table H.5 Events "CA" and "CB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CA		FAULTS THAT FAIL TRAIN A						
	OPERATOR	INSUFFICIENT BORON CONCENTRATION						1
	OPERATOR	INSUFFICIENT WATER LEVEL IN CORE FLOOD TANK A	D		ε			2
	OPERATOR	INSUFFICIENT NITROGEN PRESSURE IN CORE FLOOD TANK A	D		ε			2
	CFV-1 CHECK VALVE	DOES NOT OPEN	D		1.0 E-4	3^+, 3^-		
	CFV-2 CHECK VALVE	DOES NOT OPEN	D		1.0 E-4	3^+, 3^-		
	CFV-5F MOV	DOES NOT REMAIN OPEN (PLUGGED)	D		1.0 E-4	3^+, 3^-		
	CFV-24F	DOES NOT REMAIN CLOSED	1.0 E-5	4	4.0 E-5	3^+, 3^-		3
	MAINTENANCE	TRAIN A MAINTENANCE	.02/720	1	2.8 E-5	3^+, 3^-	M	4
					Σ = 3.7 E-4			
CB		FAULTS THAT FAIL TRAIN B						
	OPERATOR	INSUFFICEINT BORON CONCENTRATION						1
	OPERATOR	INSUFFICIENT WATER LEVEL IN CORE FLOOD TANK B	D		ε			2
	OPERATOR	INSUFFICIENT NITROGEN PRESSURE IN CORE FLOOD TANK B	D		ε			2
	CFV-3 CHECK VALVE	DOES NOT OPEN	D		1.0 E-4	3^+, 3^-		
	CFV-4 CHECK VALVE	DOES NOT OPEN	D		1.0 E-4	3^+, 3^-		
	CFV-6F MOV	DOES NOT REMAIN OPEN (PLUGGED)	D		1.0 E-4	3^+, 3^-		
	CFV-25 F	DOES NOT REMAIN CLOSED	1.0 E-5	4	4.0 E-5	3^+, 3^-		3
	MAINTENANCE	TRAIN B MAINTENANCE	.02/720	1	2.8 E-5	3^+, 3^-	M	4
					Σ = 3.7 E-4			
CM	OPERATOR	MISCALIBRATION OF TANK B PRESSURE AND LEVEL SENSORS			1.0 E-4	10^+, 10^-	H	

Table H.5 Core Flood System

QUANTIFICATION TABLES

NOTES

1 This fault would not fail the core flood tank function of cooling the core in the initial state of the accident since boron concentration is available from the BWST through the low pressure system. This fault was not further developed.

2 This parameter is maintained in the control room. Therefore, this fault was assumed to be a low probability event.

3 Tank pressure and level are verified every 8 hours via SP-300. Therefore, the fault duration time is 1/2 of 8 (=4) hours.

4 One CFT is allowed out of service for 1 hour before requirement to go to hot shutdown. Maintenance contribution was assessed assuming a frequency of 0.02 acts/month times 1/720 hr likelihood that the accident would occur during the outage.

Table H.6 Core Flood System - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
CA	3.7 E-4
CB	3.7 E-4
CM	1.0 E-4

APPENDIX K

LOW PRESSURE INJECTION AND RECIRCULATION SYSTEM

APPENDIX K LOW PRESSURE INJECTION AND RECIRCULATION SYSTEM

K.1 SYSTEM DESCRIPTION AND OPERATION

Low pressure injection and recirculation is an emergency function of the Decay Heat Removal System (DHRS). The Decay Heat Removal System (DHRS) provides both residual heat removal and emergency core cooling functions. This analysis deals only with failure of the emergency functions of the Decay Heat Removal System. Because the DHRS provides both low pressure coolant injection (LPI) and low pressure coolant recirculation (LPR), a separate fault tree analysis was performed for each mode of emergency operation.

The DHRS is utilized to provide low pressure emergency core cooling (ECC) in the event of a large LOCA. Water for the injection phase of ECC, called low pressure injection (LPI), is obtained from the BWST and injected directly into the reactor vessel. The LPR is also used to provide suction head to the high pressure pumps, when the High Pressure System is required during recirculation.

K.1.1 SYSTEM DESCRIPTION

The DHRS consists of two essentially identical trains. For ease of description, each train is separated into the following three parts: 1) pump discharge, 2) pumps and associated equipment, and 3) pump suction.

The pump discharge of each DHRS train has, as its main functional path, a separate discharge line directly into the reactor vessel through a check valve. A portion of this flow path into the vessel is shared with a core flood tank. DHRS pump discharge can also be directed to the borated water storage tank through an eight inch return line shared by both trains. Finally, DHRS flow is supplied to the suction side of the makeup pumps by each train through a remote manually operated valve for cases where the High Pressure System is required during recirculation.

The pump section of each train consists of a decay heat pump, a decay heat removal heat exchanger, and a flow control throttle valve. A minimum flow return line is provided for each pump. However, the pumps cannot operate with minimum flow for more than 15 hours without risking pump damage.

Pump suction for the DHRS can be supplied from three sources: 1) the borated water storage tank (BWST), 2) the reactor building sump, and 3) the reactor coolant system. Each train has an independent line from the BWST and RB sump while sharing a return line from the RCS. The suction lines for each DHRS train also supply suction to a reactor building spray system train and the BWST portion of the suction line (BWST side of valves DHV-34 and 35) is also shared with the makeup pump suction header.

Figure K.1 shows the LPI system valve alignment in the injection mode. The LPI system is essentially a two train redundant system. Successful operation requires flow from one operating pump (DHP-1A or 1B) be supplied to the reactor vessel. Each single stage centrifugal pump can deliver 3000 gpm at 350 foot head. The decay heat removal heat exchangers (DHHE-1A and 1B) are not required for heat removal during the injection phase.

The pumps and motor operated valves are supplied with power from the emergency AC power system. In addition, pump control power is from the emergency DC power supply. The pumps require cooling which is provided by the Decay Heat Closed Cycle Cooling System (DHCCCS). The DHCCCS, analyzed separately with the results in Section II.F, consists of two independent redundant trains, each train providing cooling to only one DHRS pump.

The BWST is the only source of water for LPI. This tank also supplies water for reactor building spray injection and high pressure injection. As illustrated in Figure K.1, each DHRS suction line supplies a spray pump and a line to the makeup pump suction header.

Figure K.2 shows the DHRS in the LPR configuration. As can be seen, LPR utilizes the same equipment as LPI with the exception of the pump suction source. Successful LPR requires the delivery of water from the reactor building sump to the reactor vessel by at least one DHRS train.

The LPR system also supplies water for two additional systems during the recirculation phase. If reactor coolant system pressure remains above the effective discharge pressure of the DHRS pumps, the makeup pumps can be used in the high pressure recirculation (HPR) mode. During HPR operation, makeup pump suction must be supplied by the DHRS pumps through DHV-11 or 12.

During the recirculation mode, reactor building heat removal is performed by the fan coolers, sprays and decay heat removal heat exchangers. The specific combinations of equipment required for successful heat removal are addressed in Section 3.0. However, the LPR system does play a role in heat removal by circulating reactor building sump water through the decay heat exchangers for heat removal.

K.1.2 SYSTEM OPERATION

Should a LOCA occur, the DHRS LPI mode is actuated by the ESAS signal which starts both pumps and sends confirmatory open signals to the normally open discharge valves on the pump discharge lines to the reactor vessel. The pumps receive a start signal when reactor coolant system pressure is less than 1500 psig and the normally open valves receive an ESAS signal to open when RCS is less than 500 psig. Although normally open, the BWST discharge valves on the suction side of the LPI pumps also receive an ESAS signal to open when RCS is less than 500 psig. The LPI system is also automatically actuated when the reactor building pressure is rising above 4 psig. Operator action is not required for actuation or operation of the DHRS in the LPI mode.

The BWST water must be recirculated once a week. This is accomplished by utilizing a DHRS pump and the DHRS return line to the BWST. This test is required to recirculate the equivalent of two volumes of the 420,000 gallon BWST which is estimated to take three hours. During this test, the LPI flow path to the reactor vessel from one DHRS pump is disabled. The test is alternated every week between LPI trains such that each LPI pump is operated for three hours once every 14 days. The technical specifications require that the reactor be shut down to hot standby if the BWST is found to be not operable and is not restored within one hour. The BWST is checked once a week for volume, boron concentration, and temperature. The temperature test frequency is increased to once a day when the ambient air temperature is less than 40^{o}F.

In addition to BWST circulation, additional checks on DHRS valve position and status are performed. Automatic actuation of pumps and valves is tested once every 18 months during refueling and the system is operated in its DHRS mode during shutdown. Should a DHRS train be found inoperable during power operation, technical specifications require it be restored within 72 hours or the plant be put in the hot shutdown mode.

When the BWST water level reaches the 'low level' (3' 9"), the emergency coolant recirculation phase is initiated and continued as long as necessary. To initiate this phase of operation, the DHRS pump suction is manually switched from the BWST to the reactor building sump. This is accomplished by first opening the RB sump valves DHV-43 and 42 when the BWST low level alarm is activated and after these two valves are verified open, the BWST outlet valves to LPI are closed.

BEST DOCUMENT AVAILABLE

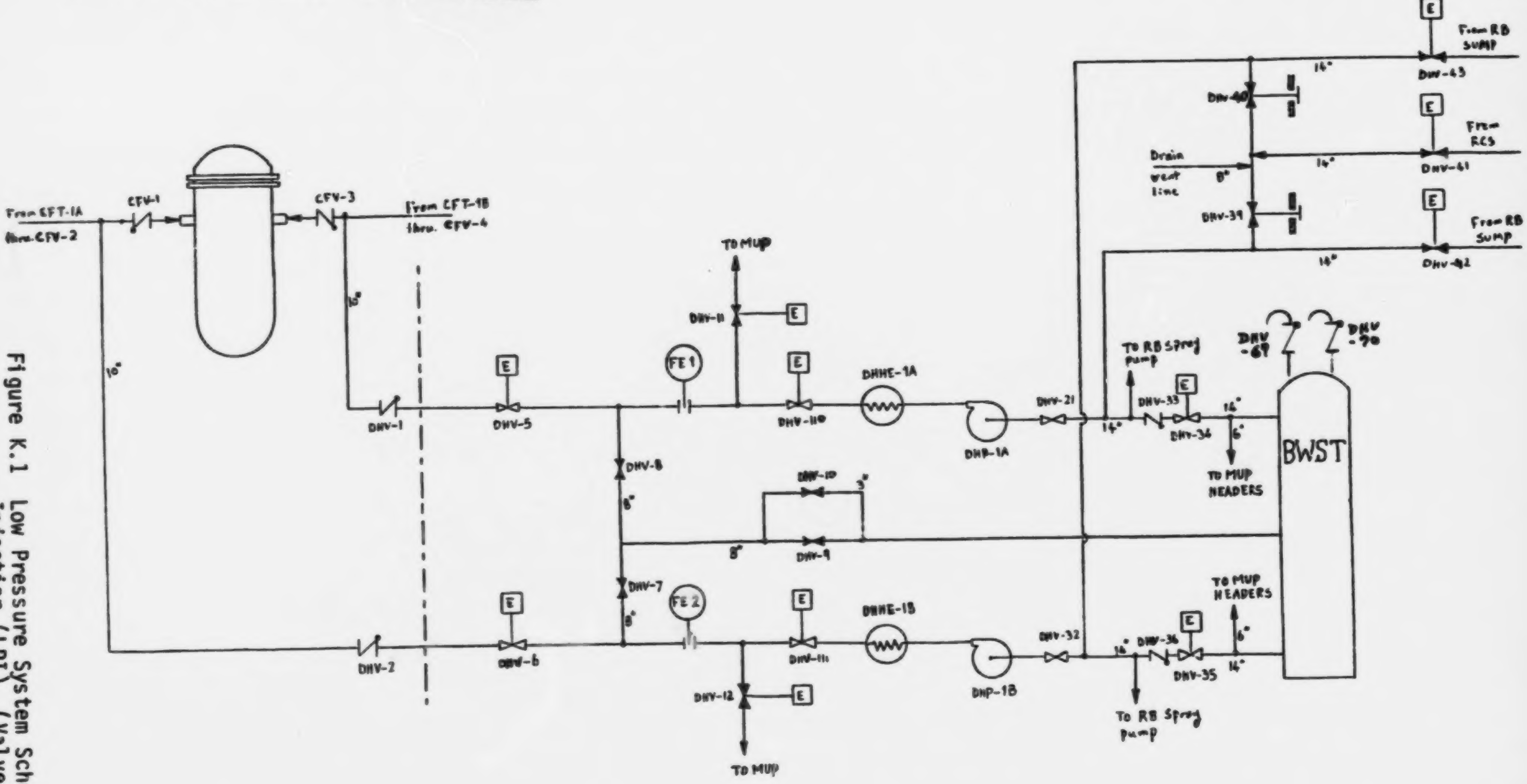

From CFT-1A
thru. CFV-2
CFV-1
CFV-3
From CFT-1B
thru. CFV-4
10"
10"
DHV-1
DHV-2
DHV-5
DHV-6
DHV-8
8"
DHV-7
8"
FE 1
FE 2
TO MUP
DHV-11
DHV-110
DHV-111
DHV-12
TO MUP
DHV-10
3"
8"
DHV-9
DHHE-1A
DHHE-1B
DHP-1A
DHP-1B
DHV-21
DHV-32
14"
TO RB Spray pump
DHV-33
DHV-34
DHV-36
DHV-35
14"
6"
TO MUP HEADERS
TO MUP HEADERS
6"
14"
14"
To RB Spray pump
BWST
DHV-69
DHV-70
E
From RB SUMP
DHV-43
14"
DHV-40
From RCS
DHV-41
14"
Drain
vent
line
8"
DHV-39
From RB SUMP
DHV-42
14"

Figure K.1 Low Pressure System Schematic Diagram - Injection (LPI) (Valve Alignment in the Injection Mode)

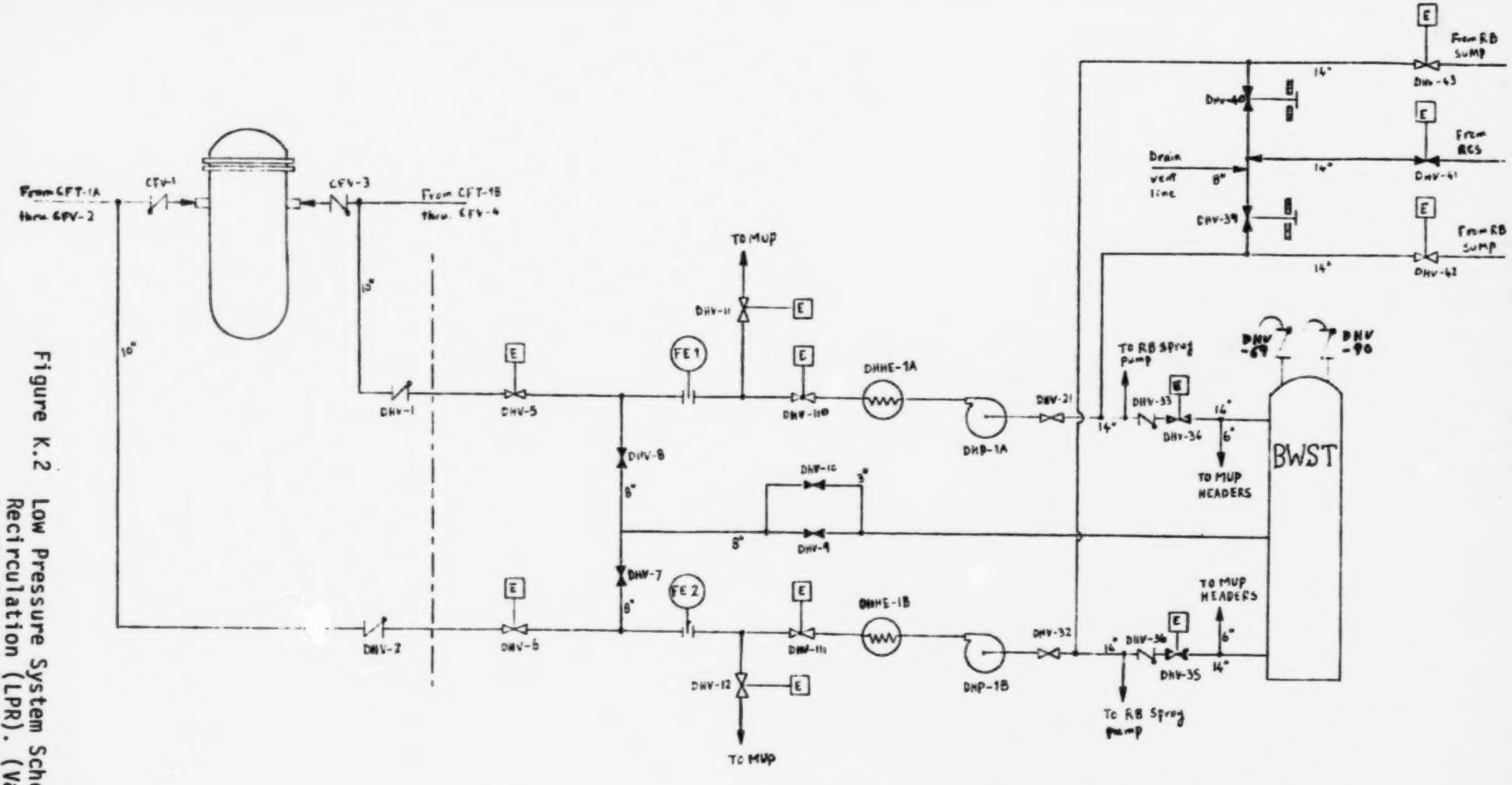

From CFT-1A
thru CFV-2
CFV-1
CFV-3
From CFT-1B
thru CFV-4
10"
10"
TO MUP
DHV-11
E
FE 1
E
DHHE-1A
DHV-1
DHV-5
DHV-110
DHP-1A
DHV-21
14"
DHV-8
8"
DHV-16
3"
8"
DHV-9
DHV-7
8"
FE 2
E
E
DHHE-1B
DHV-2
DHV-6
DHV-111
DHP-1B
DHV-32
DHV-12
TO MUP
E
From RB
sump
DHV-43
14"
DHV-40
E
From
RCS
Drain
vent
line
8"
14"
DHV-41
DHV-39
E
From RB
sump
14"
DHV-42
DHV
-69
DHV
-90
To RB Spray
pump
DHV-33
E
14"
14"
DHV-36
6"
TO MUP
HEADERS
BWST
TO MUP
HEADERS
E
6"
14"
DHV-34
DHV-35
14"
To RB Spray
pump

Figure K.2 Low Pressure System Schematic Diagram - Recirculation (LPR). (Valve Alignment in the Recirculation Mode)

BEST DOCUMENT AVAILABLE

K.2 SYSTEM SIMPLIFIED FAULT TREES

K.2.1 LPI FAULT TREE

Failure of the LPI system to supply sufficient water to the reactor vessel after a large LOCA was postulated as the top event for the simplified LPI fault tree, Figure K.3. This event implies that water from both LPI trains is not available to the reactor vessel either at the start of emergency core coolant injection or sometime during the injection phase.

The LPI system shares two ten inch lines into the reactor vessel with the core flood tanks, with one LPI train and one core flood tank (CFT) per vessel penetration. A LOCA in this line on the vessel side of CFV-1 or 3 (see Figure K.1) would also result in the failure of one CFT and one LPI train. This event was not included in the fault tree of LPI. But should it occur, the probability of failure of LPI would be the single train failure probability.

An LPI (DHRS) pump is operated once a week for BWST recirculation. During this test, either DHV-7 and 9 or DHV-8 and 9 are opened depending upon whether pump DHP-1B or 1A, respectively, is being operated. Because two valves are opened for a single pump test, failure to close both valves is postulated as a single fault event. Also, the flow path to the reactor vessel is disabled for one LPI train for the duration of this test which is estimated to require three hours.

Switching to the recirculation mode too early could also fail LPI due to insufficient NPSH in the reactor building sump. This has been identified as a plausible failure mode.

K.2.2 LPR FAULT TREE

Successful LPR operation requires the delivery of flow from one operating DHRS train. The LPR fault tree was developed for failure to supply sufficient flow from both DHRS trains when required, Figure K.4. The LPR fault tree was based upon LPI success which implies at least one operating DHRS train when LPR is required (low-level BWST alarm).

Some faults which could result in failure of one LPI train are recoverable for successful LPR. Recoverable faults are generally failures of automatic signals and mispositioned valves on the pump discharge which do not result in pump failure. The LPR fault tree includes these faults combined with the failure of the operators to recover.

Failure to properly switch to recirculation is critical. Mispositioning of either sump suction (DHV-42 and 43) or BWST outlet (DHV-34 and 35) valves could result in cavitation of LPR pumps and spray pumps. For the fault tree analysis, it is assumed that mispositioning of the valves will fail LPR and sprays in the following combinations:

Valve(s)	Misoperation	Failed Subsystem
DHV-42 and 43	Closed	LPR and Spray-Both
DHV-34 and 35	Open	LPR and Spray-Both
DHV-42	Closed	LPR and Spray-'A'
DHV-34	Open	LPR and Spray-'A'
DHV-43	Closed	LPR and Spray-'B'
DHV-35	Open	LPR and Spray-'B'

Procedure OP-404 requires that one LPR subsystem be shut down within 24 hours after the accident and additional lines from the reactor coolant system to the DHRS be opened to avoid boron precipitation. Many of the LPR components are subject to misoperation during implementation of this procedure. These items are motor operated valves DHV-5, 6, 110, 111, 42, 43, 34, and 35; locally operated manual valves DHV-8, 9, 10, and 7; and pumps DHP-1A and 1B. Misoperation of this equipment could result in failure of a single LPR subsystem or both. The specific combinations of LPR failures are included in the fault tree.

Faults associated with the suction side of the DHRS pumps are assumed to fail the pumps and necessitate pump repair for recovery. During LPR, faults on the discharge side of the pumps require only repair or reconfiguration of the faulted component or item for LPR recovery. For faults that were assessed to be recoverable see the quantification tables.

Table K.1 Simplified Fault Tree - Fault Summary (Train A (B))

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
LMVDHV5(6)P	DHV-5(6) (N.C.)	Fails to Open
LCBDHV5(6)N	DHV-5(6) Circuit Breaker	Fails Open
LXVTESTX	DHV-8(7) and -9	Open After Test
LCNV110(111)Q	DHV-110(111) Auto Controller	Closes Valve
LPMDH3A(B)R	DHP-1A(B)	Fails to Short
LPMDH3A(B)S	DHP-1A(B)	Fails to Run
LCBPU3A(B)O	Motor Contactor	Inadvertent Trip
LXVDH21(32)X	Manual Valve DHV-21(32)	Inadvertently Closed
LCBPU3A(B)N	Motor Contactor	Does Not Close
MCV00B2(1)P	Check Valve CFV-3(-1)	Fails to Open
MCV00B2(1)E	Check Valve CFV-31(-1)	Plugged
LCVDHV1(2)P	DHV-1(-2)	Fails to Open
LCVDHV1(2)E	DHV-1(-2)	Plugged
LPMDHP-1A(B)	Pump DHP-1A(B)	Fails
LCVDH33(36)P	Check Valve DHV-33(-36)	Plugged
JTKDHT1X	BWST	Leak
JTKDHT1R	BWST	Rupture
JTKDHT1E	BWST	Plug
JRVDH69P JRVDH70P	DHV 69 and DHV 70 (Coupled)	Fails to Open

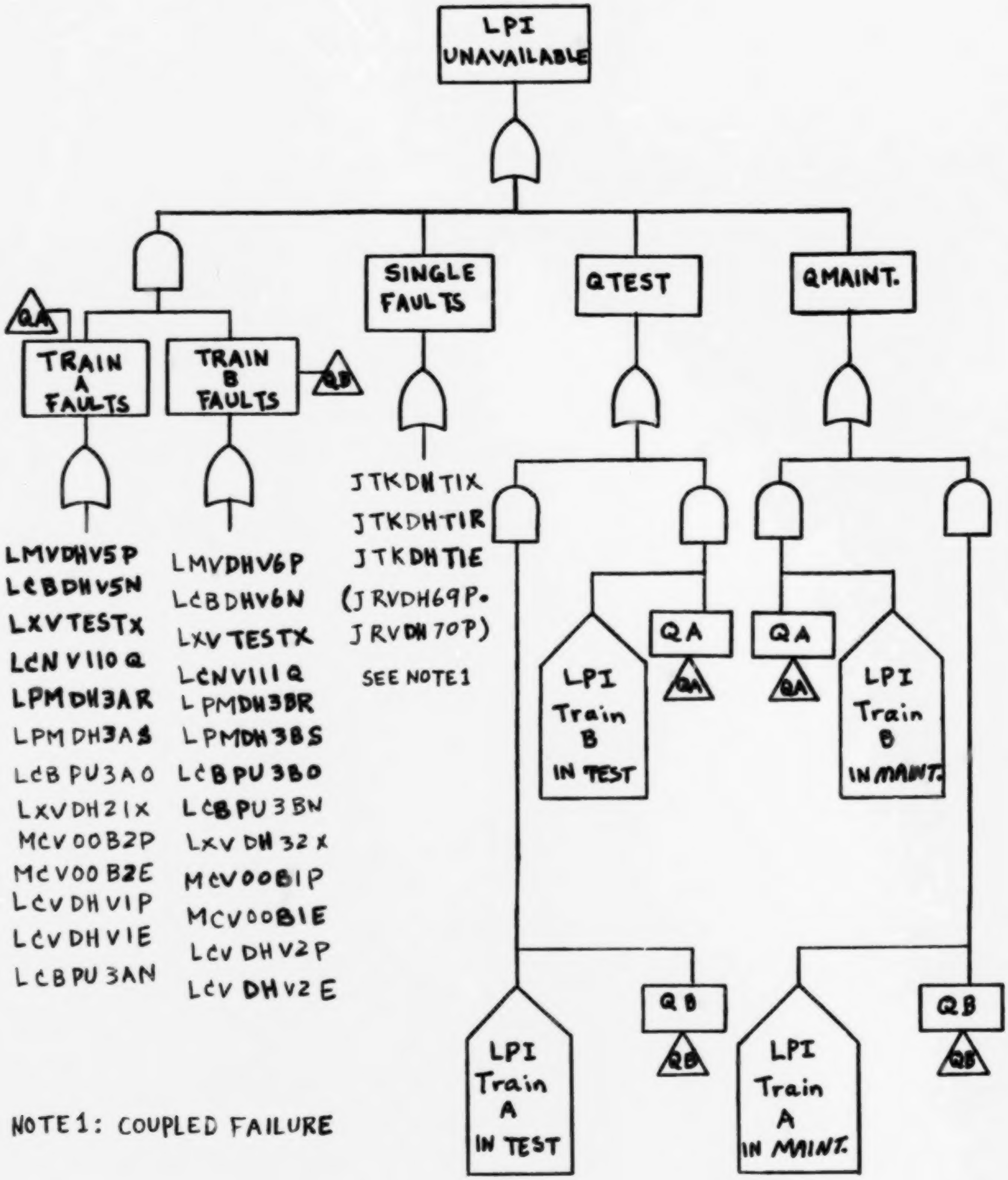

LPI UNAVAILABLE
QA
TRAIN A FAULTS
TRAIN B FAULTS
QB
SINGLE FAULTS
QTEST
QMAINT.
LMVDHV5P
LCBDHV5N
LXVTESTX
LCNV110Q
LPMDH3AR
LPMDH3AS
LCBPU3AO
LXVDH21X
MCV00B2P
MCV00B2E
LCVDHV1P
LCVDHV1E
LCBPU3AN
LMVDHV6P
LCBDHV6N
LXVTESTX
LCNV111Q
LPMDH3BR
LPMDH3BS
LCBPU3BO
LCBPU3BN
LXVDH32X
MCV00B1P
MCV00B1E
LCVDHV2P
LCVDHV2E
JTKDHTIX
JTKDHTIR
JTKDHTIE
(JRVDH69P•
JRVDH70P)
SEE NOTE 1
LPI Train B IN TEST
QA
QA
QA
QA
LPI Train B IN MAINT.
QB
QB
LPI Train A IN TEST
LPI Train A IN MAINT.
QB
QB
NOTE 1: COUPLED FAILURE

Figure K.3 Simplified Fault Tree - LPI (for the fault summary see Table K.1)

BEST DOCUMENT AVAILABLE

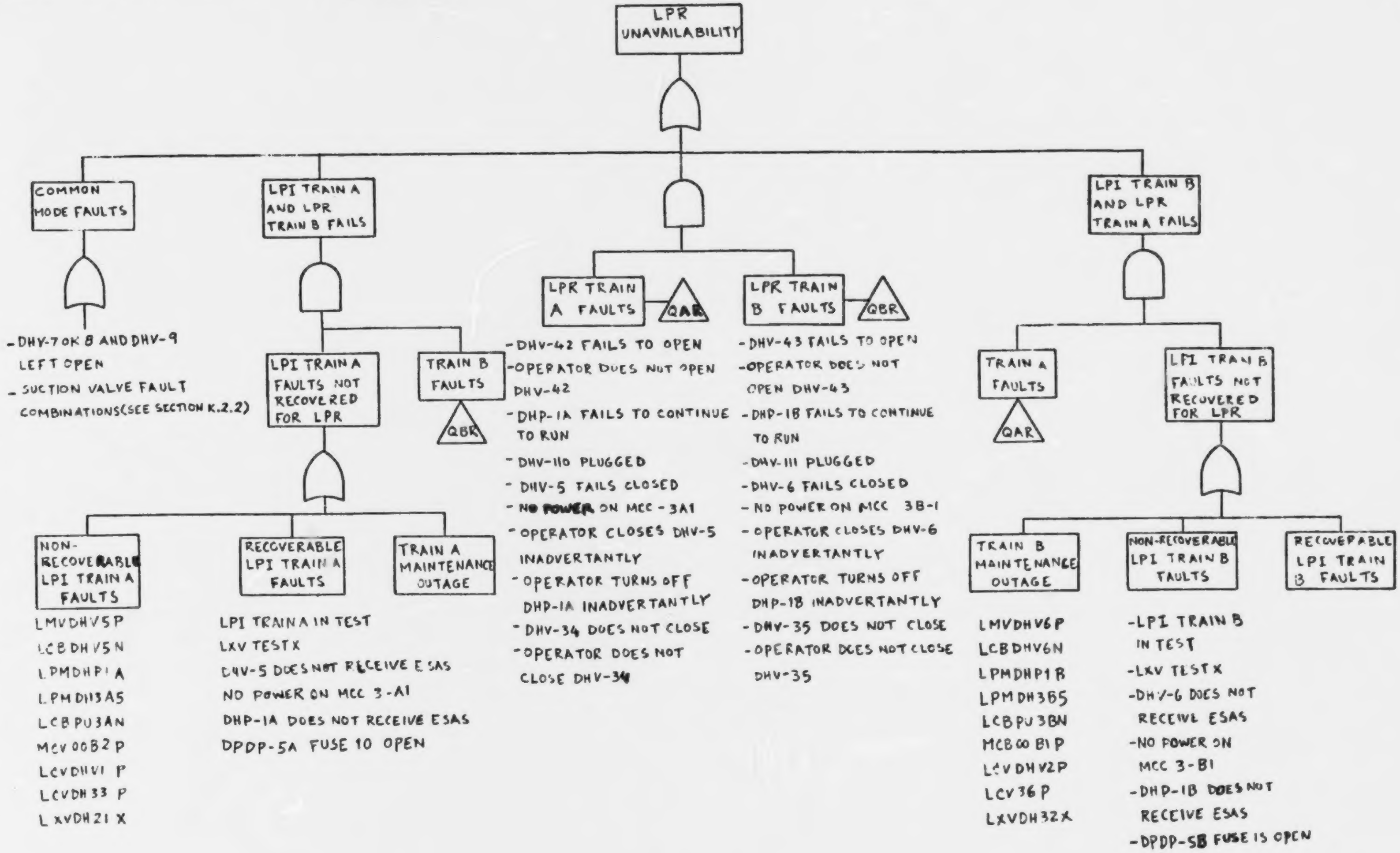

LPR UNAVAILABILITY
COMMON MODE FAULTS
-DHV-7 OK 8 AND DHV-9 LEFT OPEN
- SUCTION VALVE FAULT COMBINATIONS(SEE SECTION K.2.2)
LPI TRAIN A AND LPR TRAIN B FAILS
LPI TRAIN A FAULTS NOT RECOVERED FOR LPR
TRAIN B FAULTS
QBR
NON-RECOVERABLE LPI TRAIN A FAULTS
LMVDHV5P
LCBDHV5N
LPMDHP1A
LPMDH3A5
LCBPU3AN
MCV00B2P
LCVDHV1P
LCVDH33P
LXVDH21X
RECOVERABLE LPI TRAIN A FAULTS
LPI TRAIN A IN TEST
LXV TESTX
DHV-5 DOES NOT RECEIVE ESAS
NO POWER ON MCC 3-A1
DHP-1A DOES NOT RECEIVE ESAS
DPDP-5A FUSE 10 OPEN
TRAIN A MAINTENANCE OUTAGE
LPR TRAIN A FAULTS
QAR
-DHV-42 FAILS TO OPEN
-OPERATOR DOES NOT OPEN DHV-42
-DHP-1A FAILS TO CONTINUE TO RUN
-DHV-110 PLUGGED
-DHV-5 FAILS CLOSED
-NO POWER ON MCC-3A1
-OPERATOR CLOSES DHV-5 INADVERTANTLY
-OPERATOR TURNS OFF DHP-1A INADVERTANTLY
-DHV-34 DOES NOT CLOSE
-OPERATOR DOES NOT CLOSE DHV-34
LPR TRAIN B FAULTS
QBR
-DHV-43 FAILS TO OPEN
-OPERATOR DOES NOT OPEN DHV-43
-DHP-1B FAILS TO CONTINUE TO RUN
-DHV-111 PLUGGED
-DHV-6 FAILS CLOSED
-NO POWER ON MCC 3B-1
-OPERATOR CLOSES DHV-6 INADVERTANTLY
-OPERATOR TURNS OFF DHP-1B INADVERTANTLY
-DHV-35 DOES NOT CLOSE
-OPERATOR DOES NOT CLOSE DHV-35
LPI TRAIN B AND LPR TRAIN A FAILS
TRAIN A FAULTS
QAR
LPI TRAIN B FAULTS NOT RECOVERED FOR LPR
TRAIN B MAINTENANCE OUTAGE
LMVDHV6P
LCBDHV6N
LPMDHP1B
LPMDH3B5
LCBPU3BN
MCB00B1P
LCVDHV2P
LCV36P
LXVDH32X
NON-RECOVERABLE LPI TRAIN B FAULTS
-LPI TRAIN B IN TEST
-LXV TESTX
-DHV-6 DOES NOT RECEIVE ESAS
-NO POWER ON MCC 3-B1
-DHP-1B DOES NOT RECEIVE ESAS
-DPDP-5B FUSE IS OPEN
RECOVERABLE LPI TRAIN B FAULTS

Figure K.4 Simplified Fault Tree - LPR (For Fault Summary see Table K.1)

K.3 SYSTEM QUANTIFICATION

K.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The low pressure decay heat removal system is a two train system with a crossover that is normally valved closed. The crossover can be opened by opening manual valves, if sufficient time is available. The system is required to perform several functions, depending on the LOCA size. For the smallest LOCA, the system is required to provide suction head to the high pressure pumps during the recirculation phase. For the larger size LOCA's, the system is required to inject and recirculate cooling water directly into the reactor vessel. The low pressure system requires AC power, DC power and the DHCCCS for component cooling and decay heat removal.

For the case where offsite power is available, the LPI system unavailability is due to operator error and double failures in the low pressure trains. The operator error contribution is about a factor of two higher than the hardware contribution. This case only is applicable for the larger LOCA sizes (B_1, B_2, B_3), since it was assumed that offsite power would be available in these cases. For the smallest LOCA size (B_4) the low pressure system is not required until recirculation.

During recirculation the low pressure system is required to provide suction head to the high pressure pumps for the B_4 LOCA case. In this mode of operation, the primary contributors to low pressure system failure are operator errors. Maintenance outages also contribute to the unavailability in this case. For the larger size LOCA's, the primary contributors are also operator errors, which are about an order of magnitude larger than hardware faults.

K.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

Five modularized fault trees were constructed to quantify LPI unavailability. The top level tree shows LPI unavailability in terms of the unavailability of LPI Train A, Train B, and single faults that fail LPI. Modularized fault trees of LPI Trains A and B were constructed. For convenience of quantification, fault trees of each LPI leg to the crossover were also constructed. These fault trees apply to LOCA sizes B_1, B_2 and B_3. For the B_4 LOCA, the Low Pressure System supplies suction head to the high head pumps during the recirculation phase. Therefore, component start failures for the low head system are contained in the LPR analysis for this size LOCA.

Table K.2 shows the success criteria for LPI for the various LOCA sizes (B_1, B_2, B_3). Table K.3 shows the top event definitions for the modularized fault trees. Figures K.5 through K.7 presents the modularized fault trees. The notes to the fault trees are in Table K.4. The unavailability of each gate is shown on these trees, as well as the unavailability of the top events. Table K.5 shows the Boolean equations that represent each of these trees. Table K.6, the fault tree quantification table, shows the quantification of each gate in terms of component failure modes. The assumptions used in the quantification are described in the notes for this table. Table K.7 shows the point estimate for each gate.

Table K.2 Low Pressure Injection - Success Requirements

INITIATOR	TRAINS	NOTES
B_4 LOCA and Transient induced LOCA	1/2	1
B_3 LOCA	1/2	2
B_2 LOCA	2/2 or 1/2 with both core flood tanks operating	2, 3
B_1 LOCA	1/2 with both core flood tanks operating	2, 3

NOTES: 1. For these initiators, the Low Pressure System is actually not required until the High Pressure System is reconfigured for recirculation. The system function is more appropriately referred to as Low Head Initiation; its purpose is to boost suction pressure to the high pressure pumps. The Low Head System for the B_4-LOCA is analyzed together with B_4 - recirculation LHR. See Low Pressure Recirculation analysis.

2. For this initiator, the successful low pressure train need not correspond to a successful high pressure train.

3. Core Flood Tanks are analyzed separately.

Table K.3 Low Pressure Injection - Top Events

BOOLEAN REPRESENTATION		NOTES
B_1, B_2, B_3 - LOCAs		
LPA	Failure of low pressure Train A to provide flow to reactor vessel.	1
LPB	Failure of low pressure Train B to provide flow to reactor vessel.	
LPI	Failure of Low Pressure System to provide at least one pump flow to reactor vessel.	
LA	Low Pressure Train A failures from BWST to crossover.	
LB	Low Pressure Train B failures from BWST to crossover.	

Note: 1. The low pressure injection system is not required during the injection phase for B_4-LOCA. Faults occurring during the injection phase are included in LHR, LHA, and LHB. See quantification of the Low Pressure System during recirculation for B_4-LOCA.

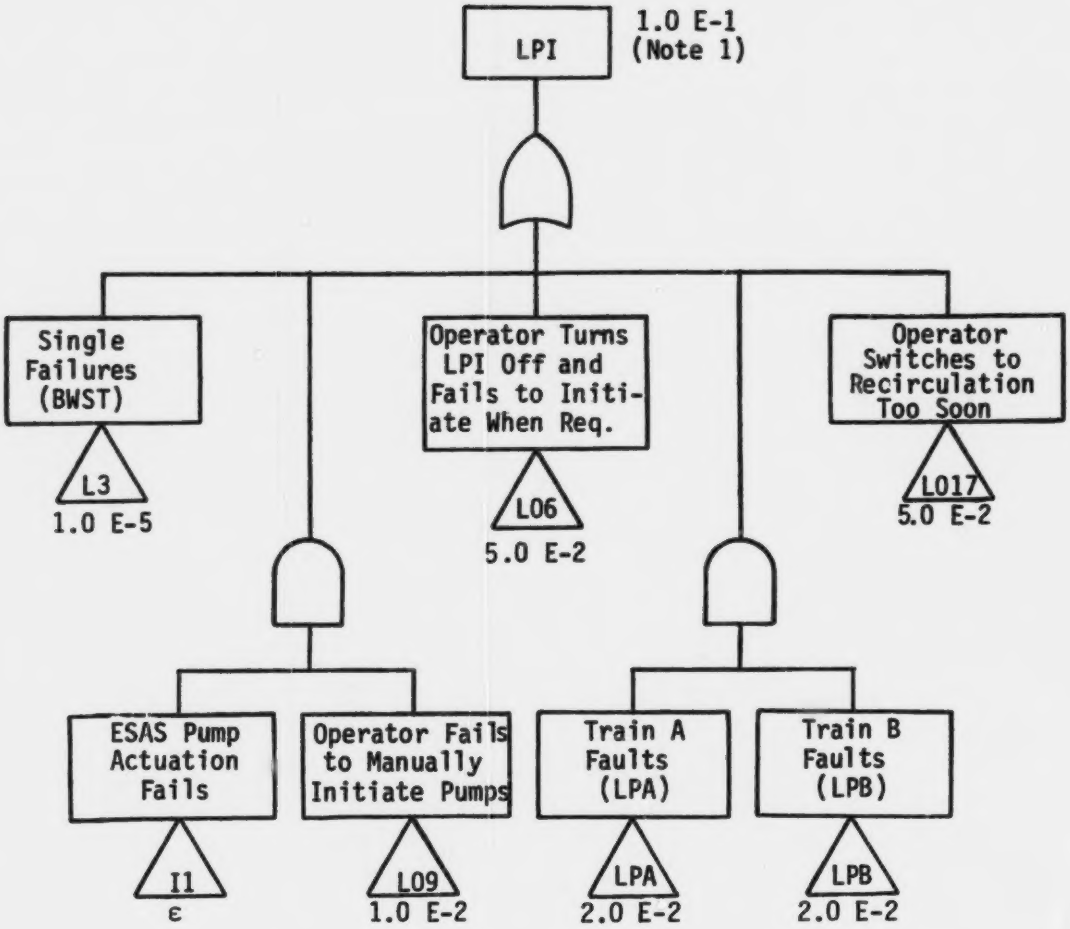

LPI
1.0 E-1
(Note 1)
Single Failures (BWST)
L3
1.0 E-5
Operator Turns LPI Off and Fails to Initiate When Req.
L06
5.0 E-2
Operator Switches to Recirculation Too Soon
L017
5.0 E-2
ESAS Pump Actuation Fails
I1
ε
Operator Fails to Manually Initiate Pumps
L09
1.0 E-2
Train A Faults (LPA)
LPA
2.0 E-2
Train B Faults (LPB)
LPB
2.0 E-2

Figure K.5 Modularized Fault Tree for Event "LPI" (B_1, B_2, B_3 LOCAs)

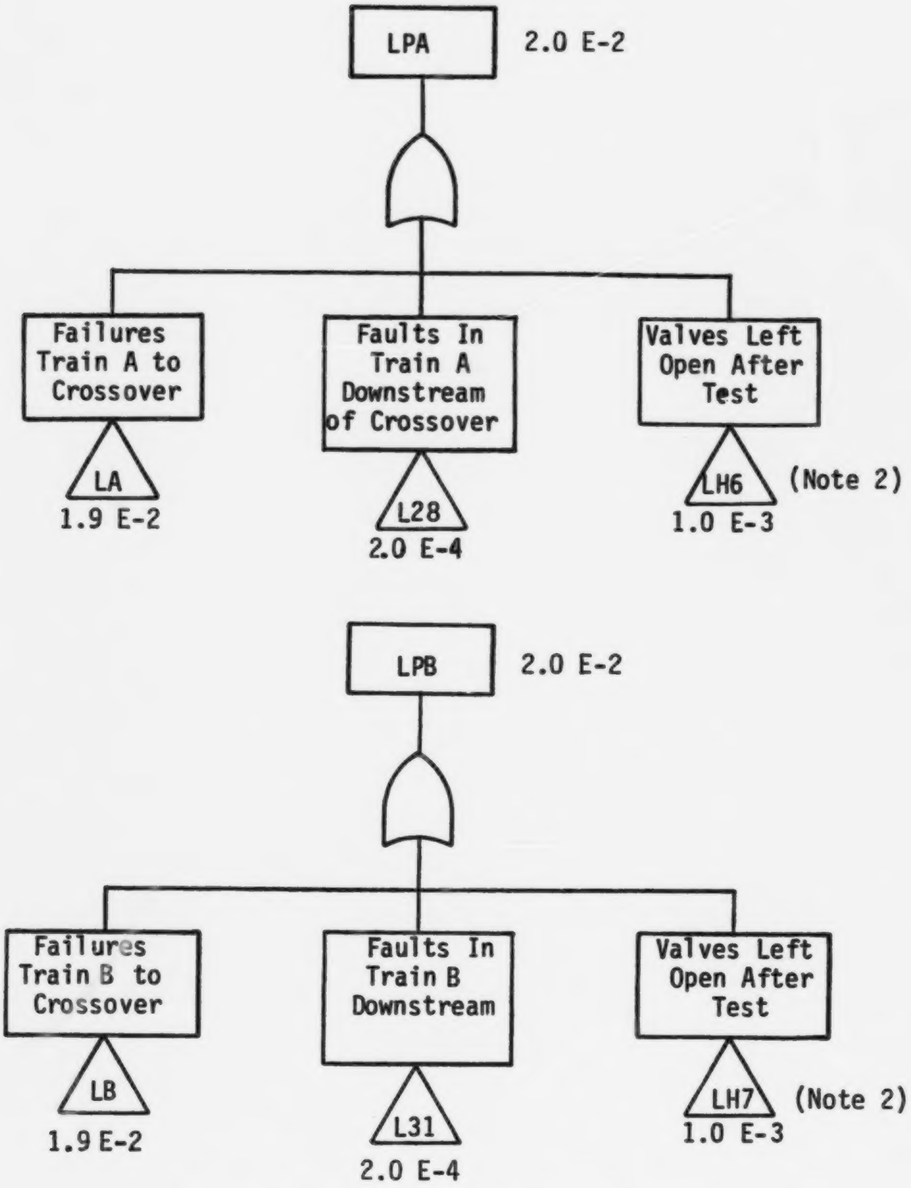

LPA
2.0 E-2
Failures Train A to Crossover
LA
1.9 E-2
Faults In Train A Downstream of Crossover
L28
2.0 E-4
Valves Left Open After Test
LH6
(Note 2)
1.0 E-3
LPB
2.0 E-2
Failures Train B to Crossover
LB
1.9 E-2
Faults In Train B Downstream
L31
2.0 E-4
Valves Left Open After Test
LH7
(Note 2)
1.0 E-3

Figure K.6 Modularized Fault Trees for Events "LPA" and "LPB" (B_1, B_2, B_3 LOCAs)

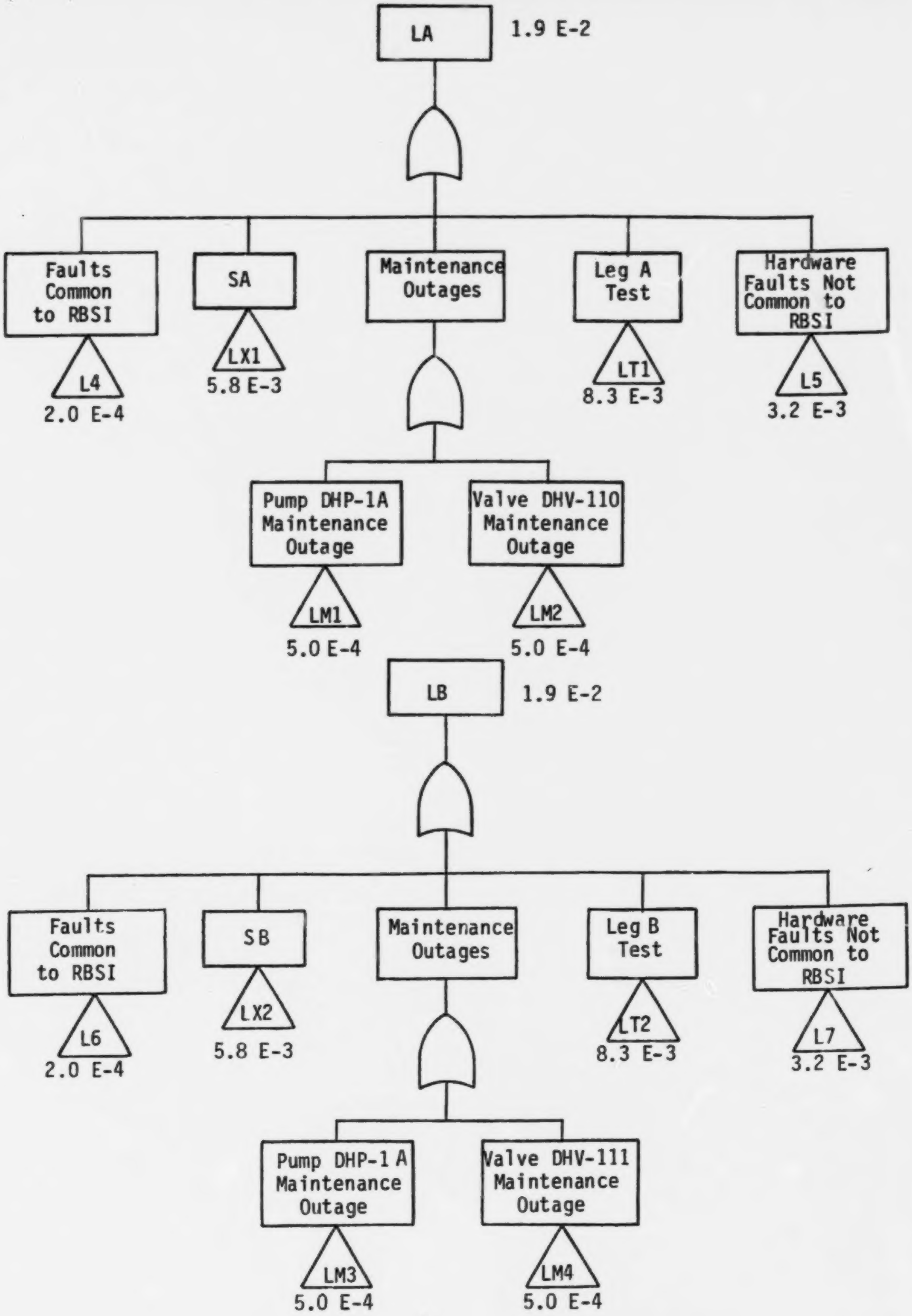

LA
1.9 E-2
Faults Common to RBSI
L4
2.0 E-4
SA
LX1
5.8 E-3
Maintenance Outages
Leg A Test
LT1
8.3 E-3
Hardware Faults Not Common to RBSI
L5
3.2 E-3
Pump DHP-1A Maintenance Outage
LM1
5.0 E-4
Valve DHV-110 Maintenance Outage
LM2
5.0 E-4
LB
1.9 E-2
Faults Common to RBSI
L6
2.0 E-4
SB
LX2
5.8 E-3
Maintenance Outages
Leg B Test
LT2
8.3 E-3
Hardware Faults Not Common to RBSI
L7
3.2 E-3
Pump DHP-1 A Maintenance Outage
LM3
5.0 E-4
Valve DHV-111 Maintenance Outage
LM4
5.0 E-4

Figure K.7 Modularized Fault Trees for Events "LA" and "LB" (B_1, B_2, B_3 LOCAs)

Table K.4 Low Pressure Injection (B_3, B_2, B_1-LOCAs)

FAULT TREES (LPA, LPB, LPI)

NOTES

1 LPA, LPB, and LPI are failure of the low pressure injection system during emergency core cooling initiation.

2 Operator fails to close DHV-8,9 which fails Train A of LPI. Operator fails to close DHV-7,9 which fails Train B of LPI. These acts were assessed as a triple common mode human fault that fails both trains of LPI.

Table K.5 Low Pressure Injection (B_1, B_2, B_3-LOCAs)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS — NOTES

$LPI = L3 + L06 + I1 \cdot L09 + L017 + LPA \cdot LPB$

$LPA = L28 + LH6 + LA$ — 2

$LPB = L31 + LH7 + LB$ — 2

INTERMEDIATE EVENTS

$LA = L4 + L5 + LT1 + LM1 + LM2 + LX1$ — 2

$LB = L6 + L7 + LT2 + LM3 + LM4 + LX2$ — 2

$LX1 = ACA + DCA + DA$

$LX2 = ACB + DCB + DB$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENTS

$$\begin{aligned} LPI = {} & L3 + L06 + I1 \cdot L09 + L017 + (L4 \cdot L6) + (L5 \cdot L7) + (ACA \cdot ACB) + \\ & + DA \cdot DB + (L28 \cdot L31) + (LH6 \cdot LH7) + L4 \cdot L7 + L5 \cdot L6 + \\ & + ACA \cdot (L6 + L7 + LT2 + LM3 + LM4 + DB) + (L4 + L5) \cdot (LT2 + LM3 + LM4) + \\ & + ACB \cdot (L4 + L5 + LT1 + LM1 + LM2 + DA) + (L6 + L7) \cdot (LT1 + LM1 + LM2) + \\ & + DA \cdot (L6 + L7 + LT2 + LM3 + LM4) + DB \cdot (L4 + L5 + LT1 + LM1 + LM2) + \\ & + LA \cdot (L31 + LH7) + LB \cdot (L28 + LH6) \end{aligned}$$

(1,2,3,4)

$LA = L4 + L5 + LT1 + LM1 + LM2 + LX1$

$LB = L6 + L7 + LT2 + LM3 + LM4 + LX2$

Table K.5 Boolean Equations (LOCAs B_1, B_2, B_3)

NOTES

1 The event LH6·LH7 was evaluated as a triple common mode human error of leaving valves DHV-7, DHV-8, DHV-9 in the wrong position (open) after test.

2 The terms LPA·LPB and LA·LB contain hardware components that were assumed to have coupled failure modes. See quantification tables.

3 It was assumed that no recovery is possible for legs in test when the low pressure injection system is required for the injection phase.

4 Terms representing simultaneous outages in both legs are omitted since they are prohibited by Technical Specifications.

Table K.6 (1/4) Event "LPI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L3		SINGLE FAILURES	D		1.0 E-5	$2^+, 2^-$	B	
	BWST	LEAKS			ε			1
	BWST	RUPTURE			ε			1
	BWST	PLUG			ε			1
	BWST	TWO REDUNDANT VACUUM BREAKERS FAIL TO OPEN	D	(1.E-4)(0.1)	1.0 E-5	$2^+, 2^-$	B	2
					Σ=1.0 E-5			
LO6	OPERATOR	TURNS LPI OFF AND FAILS TO INITIATE	D		5.0 E-2	$3^+, 10^-$	O	12, 20
LO9	OPERATOR	FAILS TO MANUALLY INITIATE PUMPS	D		1.0 E-2	$3^+, 10^-$	O	11
I1	ESAS(ILB3·ILB3)	FAILS TO ACTUATE BOTH PUMPS			ε			
LO17	OPERATOR	SWITCHES TO RECIRCULATION TOO SOON	D		5.0 E-2	$3^+, 10^-$	O	20
L4·L6		EVENT INCLUDING COUPLED VALVE FAILURES DHV-33, DHV-34, DHV-35, DHV-36			1.0 E-5	$2^+, 2^-$	B	3
L5·L7		EVENT INCLUDING COUPLED PUMP FAILURES DHP-1A, DHP-1B			1.0 E-4	$2^+, 2^-$	B	4
DA·DB		EVENT INCLUDING COUPLED FAILURES IN BOTH TRAINS OF DHCCCS. SEE DHCCCS FAULT TREE QUANTIFICATION TABLE						
L28·L31		EVENT INCLUDING COUPLED CHECK VALVE FAILURES CFV-1, CFV-3			2.0 E-5	$2^+, 2^-$	B	5
LH6·LH7	HUMAN	COMMON MODE HUMAN FAILURE OF LEAVING VALVES DHV-7, 8, 9 IN OPEN POSITION AFTER TEST (SEE TABLE K.6)			1.0 E-5	$3^+, 3^-$	H	6

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table K.6 (2/4) Events "LPA" and "LPB" Quantification (Note 9)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L28		FAULTS IN TRAIN A DOWNSTREAM OF CROSSOVER			2.0 E-4			
	CHECK VALVE DHV-1	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	CHECK VALVE CFV-3	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		10
					Σ =2.0 E-4			
LH6	HUMAN	VALVES DHV-8, DHV-9 LEFT OPEN AFTER TEST	D		1.0 E-3	3^+, 3^-	H	13
L31		FAULTS IN TRAIN B DOWNSTREAM OF CROSSOVER			2.0 E-4			
	CHECK VALVE DHV-2	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	CHECK VALVE CFV-1	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		10
					Σ =2.0 E-4			
LH7	HUMAN	VALVE DHV-7, DHV-9 LEFT OPEN AFTER TEST	D		1.0 E-3	3^+, 3^-	H	13

Table K.6 (3/4) Event "LA" Quantification (Note 14)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L4		FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
	DHV-34	VALVE PLUGGED	D		1.0 E-4	$3^+, 3^-$		
	CHECK VALVE DHV-33	FAILS TO OPEN (PLUGGED)	D		1.0 E-4	$3^+, 3^-$		
					Σ=2.0 E-4			
L5		HARDWARE FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION			3.2 E-3	$3^+, 3^-$ $3^+, 3^-$	H H	
	DHP-1A	PUMP FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	DHP-1A CIRCUIT BREAKERS	CIRCUIT BREAKER FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	DPDP-5A FUSE 10	OPEN	1.0 E-6	168	1.7 E-4	$3^+, 3^-$		15
	DHV-21	MANUAL VALVE LEFT CLOSED	D		1.0 E-3	$3^+, 3^-$	H	16
					Σ=3.2 E-3			
LM1	DHP-1A	OUT OF SERVICE	.02/720	18	5.0 E-4	$3^+, 3^-$	H	
LM2	DHV-110	OUT OF SERVICE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	
LT1		LEG A IN TEST	2/720	3	8.3 E-3			17
LX1		SYSTEM INTERFACE FAULTS			5.8 E-3			
ACA		AC TRAIN A INSUFFICIENT POWER						
		NON LOSS OF OFFSITE POWER			ε			18, 19
DCA		DC TRAIN A INSUFFICIENT POWER						
		NON LOSS OF OFFSITE POWER			ε			
								7
DA		DHCCCS INSUFFICIENT COOLING						
		NON LOSS OF OFFSITE POWER			5.8 E-3			
					Σ =5.8 E-3			8

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table K.6 (4/4) Event "LB" Quantification (Note 14)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L6		FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
	DHV-35	VALVE PLUGGED	D		1.0 E-4	$3^+, 3^-$		
	CHECK VALVE DHV-36	FAILS TO OPEN (PLUGGED)	D		1.0 E-4	$3^+, 3^-$		
					Σ=2.0 E-4			
L7		HARDWARE FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION			3.2 E-3	$3^+, 3^-$	H	
	DHP-1B	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	DHP-1B CIRCUIT BREAKER	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	DPDB-5B FUSE 10	OPEN	1.0 E-6	168	1.7 E-4	$3^+, 3^-$		15
	DHV-32	MANUAL VALVE LEFT CLOSED	D		1.0 E-3	$3^+, 3^-$	H	16
					Σ=3.2 E-3			
LM3	DHP-1B	OUT OF SERVICE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	
LM4	DHV-111	OUT OF SERVICE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	
LT2		LEG B IN TEST	2/720	3	8.3 E-3			17
LX2		SYSTEM INTERFACE FAULTS						
ACB		AC TRAIN B INSUFFICIENT POWER			5.8 E-3			
		NON LOSP			ε			
DCB		DC TRAIN B INSUFFICIENT POWER						
		NON LOSP			ε			
								7
DB		DHCCCS INSUFFICIENT COOLING						
		NON LOSP			5.8 E-3			
					Σ=5.8 E-3			

Table K.6 (1/2) Fault Tree Quantification (B_1, B_2, B_3-LOCAs)

NOTES

1 BWST level is monitored, so these faults could not exist for any appreciable length of time before discovery and corrective action. Therefore, they were assessed as negligible contributors (ϵ).

2 This fault was assessed as a hardware common mode failure of 2 vacuum breakers failing to open when required. A failure probability of 1.0 E-4 (check valve demand failure rate) was used as the single vacuum breaker failure mode. A coupling coefficient (β-factor) of 0.1 was used as the conditional probability of failure of the second given failure of the first.

3 The event L4·L6 was evaluated assuming coupled failure between valves DHV-33, 34, 35, and 36. A coupling coefficient (conditional probability of failure of one valve, given failure of the other valve, or β-factor) of 0.1 was assumed.

4 The event L5·L7 was evaluated assuming coupled failures between pumps DHP-1A and DHP-1B. A coupling coefficient (conditional probability of failure of one pump, given failure of the other pump, or β-factor) of 0.1 was assumed.

5 The event L28·L31 was evaluated assuming coupled failures between check valves CFV-1 and CFV-3. These component failures were assumed to be coupled because they see the same pressure differential. A coupling coefficient (conditional probability of failure of one check valve, given failure of the other, or β-factor) of 0.1 was assumed.

6 This common error was assessed as 1.0 E-3 (frequency) for leaving 1 pair of valves in incorrect position after test with an additional frequency of 1.0 E-2 for leaving the third valve in incorrect position. The two acts were assumed to be independent.

7 See DC-power quantification tables.

8 The event DA contains event ACA.

Table K.6 (2/2) Fault Tree Quantification (B_1, B_2, B_3-LOCAs) (Cont.)

NOTES

9 LPA (LPB) includes only those faults that fail Train A(B) of LPI to the reactor vessel.

10 Check valve CFV-3(1) failure assumed coupled with check valve CFV-1(3) failure; see event L28·L31 in LPI quantification table.

11 If ESAS actuation of pump DHP-1H(B) fails, operator can recover by manually initiating. A frequency of 1.0 E-2 was assumed to be the probability of failure to recover.

12 Operator terminates LPI. When LPI is required at a later time, initiation is manual.

13 Common mode human error of leaving two manual valves in wrong position after test. Assessed as 1.0 E-2 for the basic fault and a coupling coefficient of 0.1.

14 Only faults upstream of crossover contribute to LA or LB.

15 Fault duration time is 1/2 of 2 weeks, since fuse is tested bi-weekly via pump tests.

16 This fault represents the human error of leaving the valve closed following pump maintenance. The unavailability is estimated as follows: (0.02 maintenance acts per month) X (1.0 E-2 per act) X (360/720 months fault duration).

17 Each leg is operated for about 3 hours every two weeks to recirculate BWST water.

18 See appropriate fault tree analysis.

19 For loss of offsite power transients, this fault is assumed to be recovered, even if the diesel fails, by the time the system is required.

20 This human error was evaluated using THERP tree analysis as described in NUREG/CR-1278.

Table K.7 (1/2) LPI - Quantification Summary (B_1, B_2, B_3 LOCAs)

BOOLEAN VARIABLE	POINT ESTIMATES
L3	1.0 E-5
L06	5.0 E-2
L09	1.0 E-2
I1	ε
L017	5.0 E-2
L4·L6	1.0 E-5
L5·L7	1.0 E-4
L28·L31	2.0 E-5
LH6·LH7	1.0 E-5
L28	2.0 E-4
LH6	1.0 E-3
L31	2.0 E-4
LH7	1.0 E-3
L4	2.0 E-4
L5	3.2 E-3
LM1	5.0 E-4
LM2	5.0 E-4
LT1	8.3 E-3
ACA	ε* 3.2 E-2**
DCA	ε* 3.2 E-3**
DA	5.8 E-3* 3.8 E-2**
L6	2.0 E-4

Table K.7 (2/2) LPI - Quantification Summary (B_1, B_2, B_3 LOCAs)

BOOLEAN VARIABLE	POINT ESTIMATES
L7	3.2 E-3
LM3	5.0 E-4
LM4	5.0 E-4
LT2	8.3 E-3
ACB	ε* 3.2 E-2**
DCB	ε* 3.2 E-3
DB	5.8 E-3* 3.8 E-2**

*Offsite power available
**Offsite power not available

K.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

Modularized fault trees for Low Pressure System failure during the recirculation phase were developed for the four LOCA size accident initiators. For the smallest LOCA size (B_4) the Low Pressure System is not required until the recirculation phase. At recirculation this system is required to boost the suction head of the high pressure pumps. Modularized fault trees were constructed for failure to provide suction head to each of the high pressure pumps, and failure to provide suction head to either of the high head pumps. For the other LOCA sizes, the LPR is required to inject water into the reactor vessel and remove heat during the recirculation phase. Four modularized fault trees were constructed for failure of this function, corresponding to failure of combinations of each train in injection and recirculation leading to failure of both trains.

Table K.8 shows the success criteria for each LOCA size, Table K.9 shows the top event definitions for each of the modularized fault trees, and Figures K.8 through K.14 show the modularized fault trees. The unavailability or unreliability of each gate is shown on these trees, as well as the unreliability of the top events. Tables K.10 and K.11 show the Boolean equations that represent the fault trees. Table K.12, the fault tree quantification tables, show the quantification of each gate in terms of component failure modes. The notes for this table explain the assumptions that were made in the quantification. Tables K.13 and K.14 show the point estimates of each gate.

Table K.8 Low Pressure Recirculation - Success Requirements

INITIATOR	TRAINS	NOTES
B_4 LOCA and Transient induced LOCA	1/2 trains with associated high pressure train	1,2,3
B_3 LOCA	1/2	4,5,6
B_2 LOCA	1/2	4,5,6
B_1 LOCA	1/2	4,5,6

Table K.8 Low Pressure Recirculation - Success Requirements

NOTES

1 For the B$_4$-LOCA failures of pumps and valves to change state (e.g., alignment to low head injection) which would ordinarily be included in the anlysis of low head injection, are included in low head recirculation. This is because the low pressure system is not required until the recirculation phase.

2 The low pressure trains are required to boost the suction head of the high pressure trains. The associated trains of the low pressure and high pressure systems are required to provide a flow path between the pump and the reactor vessel. The associated DHCCCS-trains are also required to provide component cooling and decay heat removal.

3 A possible second success path is 1/2 high pressure recirculation trains with associated low pressure train with 1/3 fan coolers operating. However, this success path implies that component cooling is provided by the DHCCCS and only the decay heat removal function of the DHCCCS is unavailable. Such a failure mode for the DHCCCS is considered to be very unlikely. Therefore, only the first success criterion was used in the analysis.

4 The success path is 1/2 low pressure recirculation trains with associated DHCCCS-trains for component cooling and decay heat removal. The alternate success path of 1/2 LPR-trains with 1/3 fan coolers was not considered for the reasons given in Note 2.

5 For this initiator, the successful low pressure train need not correspond to a successful high pressure train.

6 Assumes system success in the injection phase.

Table K.9 Low Pressure Recirculation - Top Events

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
B_4 - LOCA		
LHA	Failure of low pressure system to provide flow to suction of high pressure Train A during recirculation	1
LHB	Failure of low pressure system to provide flow to suction of high pressure Train B during recirculation.	1
LHR	Failure of low pressure system to provide flow to suction of at least one high pressure train during recirculation.	1
OTHER LOCAs (B_1, B_2, B_3)		
LPR	Failure of low pressure system to provide at least one pump flow to reactor vessel during recirculation.	2
LRR	Failure of both low pressure system trains to provide flow to the reactor vessel during recirculation.	2
LIR	Failure of low pressure system Train A during injection and of Train B during recirculation to provide flow to reactor vessel.	2
LRI	Failure of low pressure system Train B during injection and of Train A during recirculation to provide flow to reactor vessel.	2

NOTES: 1. This event includes failure of the pumps to start, and failure of the valves to align for injection.

2. This event assumes success or recovery during the injection phase.

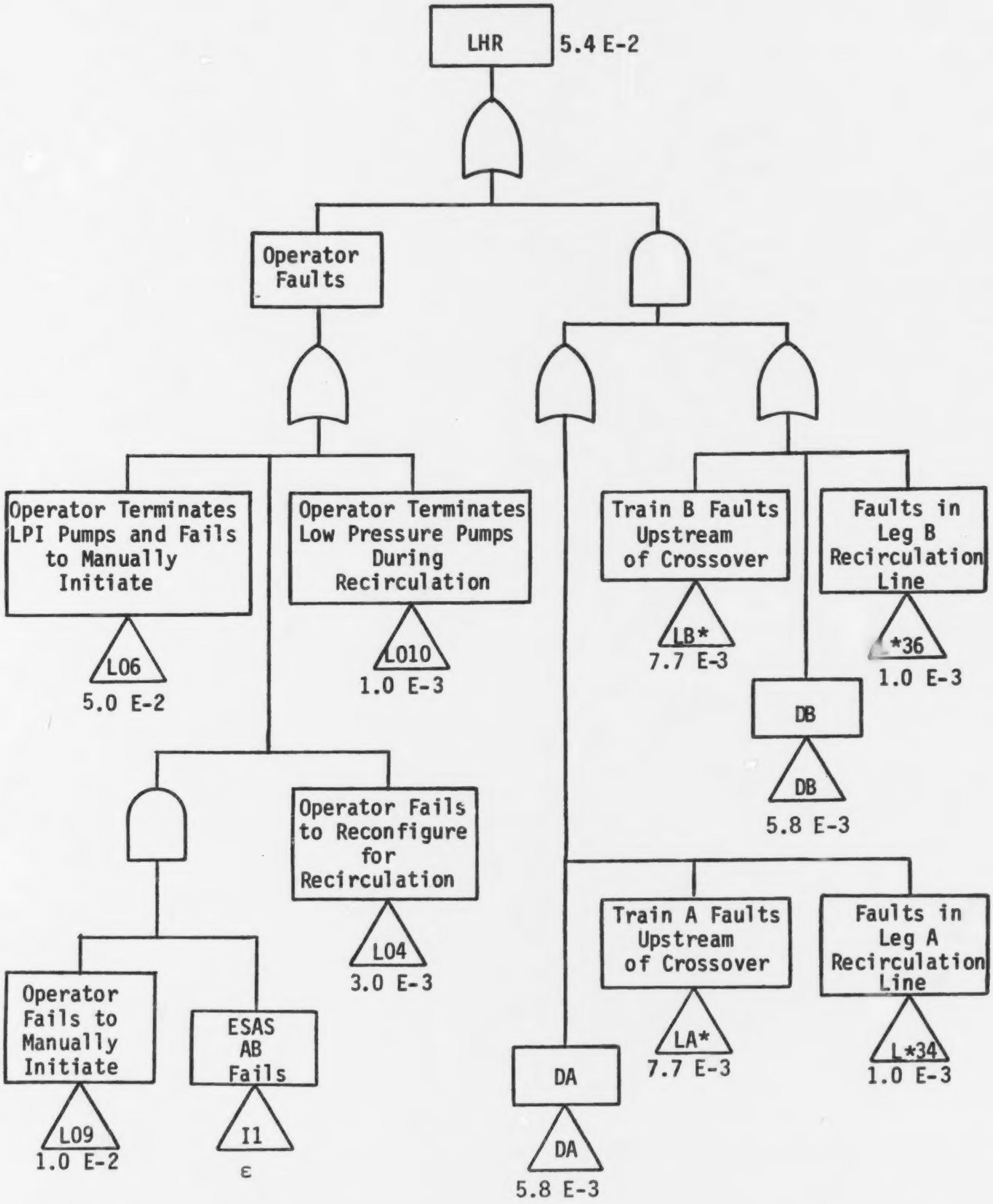

LHR
5.4 E-2
Operator Faults
Operator Terminates LPI Pumps and Fails to Manually Initiate
L06
5.0 E-2
Operator Terminates Low Pressure Pumps During Recirculation
L010
1.0 E-3
Operator Fails to Reconfigure for Recirculation
L04
3.0 E-3
Operator Fails to Manually Initiate
L09
1.0 E-2
ESAS AB Fails
I1
ε
Train B Faults Upstream of Crossover
LB*
7.7 E-3
Faults in Leg B Recirculation Line
L*36
1.0 E-3
DB
DB
5.8 E-3
Train A Faults Upstream of Crossover
LA*
7.7 E-3
Faults in Leg A Recirculation Line
L*34
1.0 E-3
DA
DA
5.8 E-3

Figure K.8 Modularized Fault Tree for Event "LHR" (B_4 LOCA)

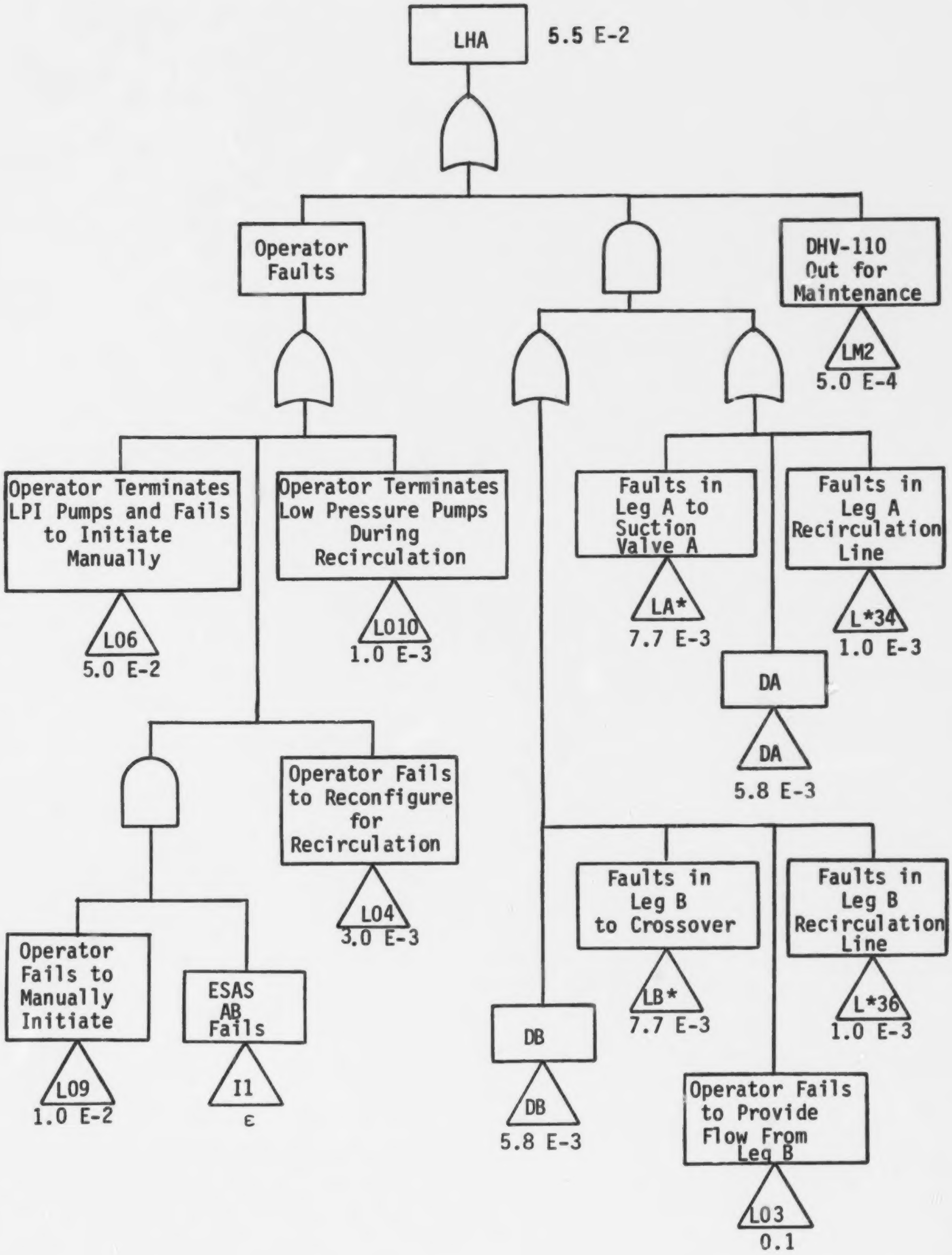

LHA
5.5 E-2
Operator Faults
DHV-110 Out for Maintenance
LM2
5.0 E-4
Operator Terminates LPI Pumps and Fails to Initiate Manually
L06
5.0 E-2
Operator Terminates Low Pressure Pumps During Recirculation
L010
1.0 E-3
Faults in Leg A to Suction Valve A
LA*
7.7 E-3
Faults in Leg A Recirculation Line
L*34
1.0 E-3
DA
DA
5.8 E-3
Operator Fails to Reconfigure for Recirculation
L04
3.0 E-3
Faults in Leg B to Crossover
LB*
7.7 E-3
Faults in Leg B Recirculation Line
L*36
1.0 E-3
Operator Fails to Manually Initiate
L09
1.0 E-2
ESAS AB Fails
I1
ε
DB
DB
5.8 E-3
Operator Fails to Provide Flow From Leg B
L03
0.1

Figure K.9 Modularized Fault Tree for Event "LHA" (B_4 LOCA)

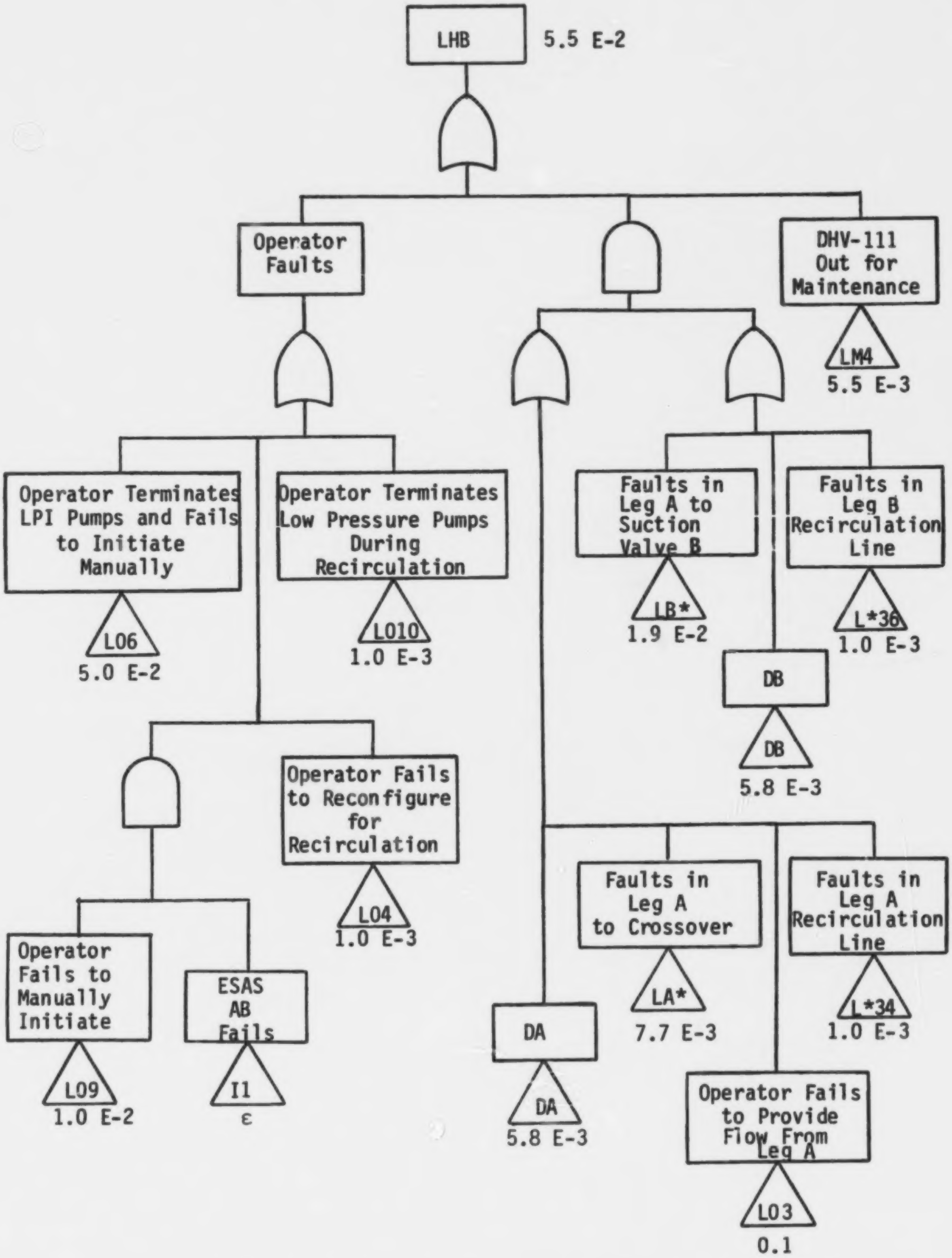

LHB
5.5 E-2
Operator Faults
DHV-111 Out for Maintenance
LM4
5.5 E-3
Operator Terminates LPI Pumps and Fails to Initiate Manually
L06
5.0 E-2
Operator Terminates Low Pressure Pumps During Recirculation
L010
1.0 E-3
Faults in Leg A to Suction Valve B
LB*
1.9 E-2
Faults in Leg B Recirculation Line
L*36
1.0 E-3
DB
DB
5.8 E-3
Operator Fails to Reconfigure for Recirculation
L04
1.0 E-3
Operator Fails to Manually Initiate
L09
1.0 E-2
ESAS AB Fails
I1
ε
Faults in Leg A to Crossover
LA*
7.7 E-3
Faults in Leg A Recirculation Line
L*34
1.0 E-3
DA
DA
5.8 E-3
Operator Fails to Provide Flow From Leg A
L03
0.1

Figure K.10 Modularized Fault Tree for Event "LHB" (B_4 LOCA)

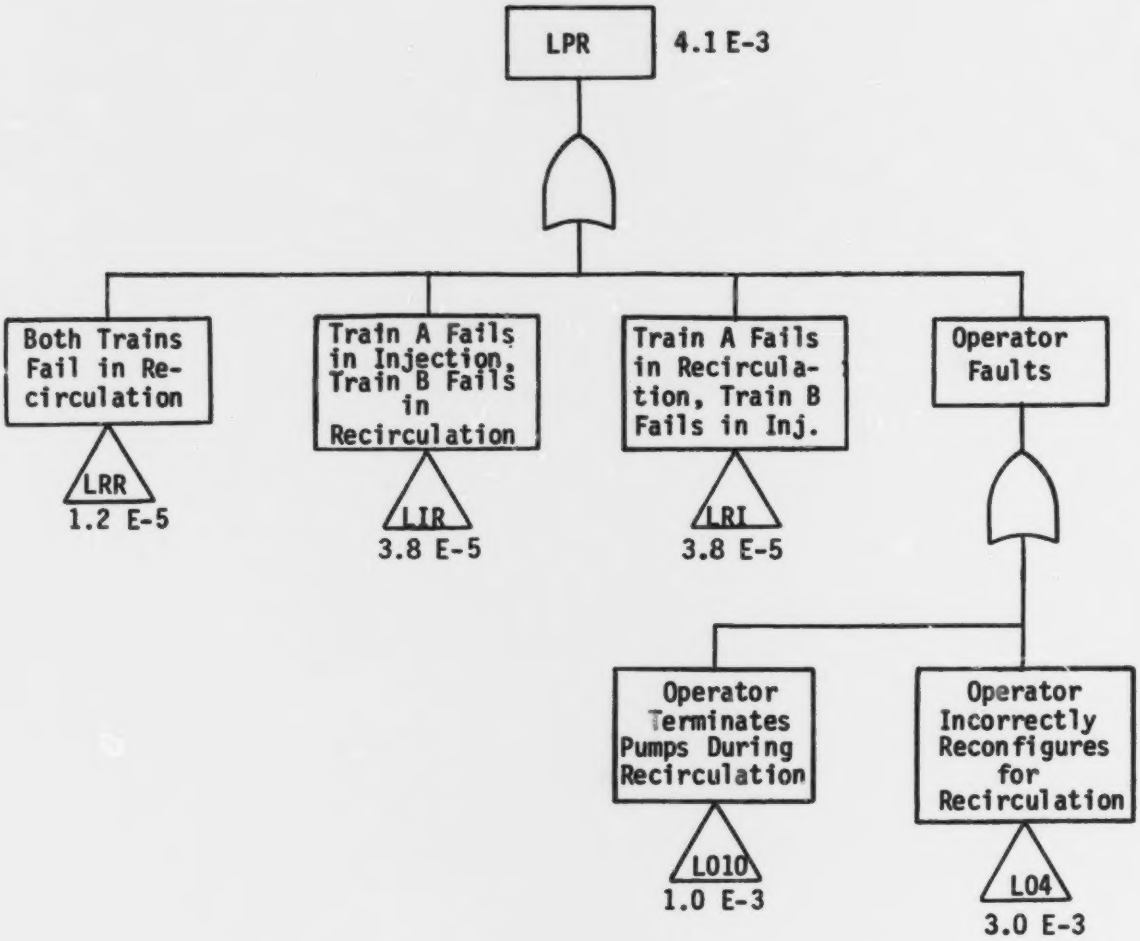

LPR
4.1 E-3
Both Trains Fail in Recirculation
LRR
1.2 E-5
Train A Fails in Injection, Train B Fails in Recirculation
LIR
3.8 E-5
Train A Fails in Recirculation, Train B Fails in Inj.
LRI
3.8 E-5
Operator Faults
Operator Terminates Pumps During Recirculation
LO10
1.0 E-3
Operator Incorrectly Reconfigures for Recirculation
LO4
3.0 E-3

Figure K.11 Modularized Fault Tree for Event "LPR" (B_1, B_2, B_3 LOCAs)

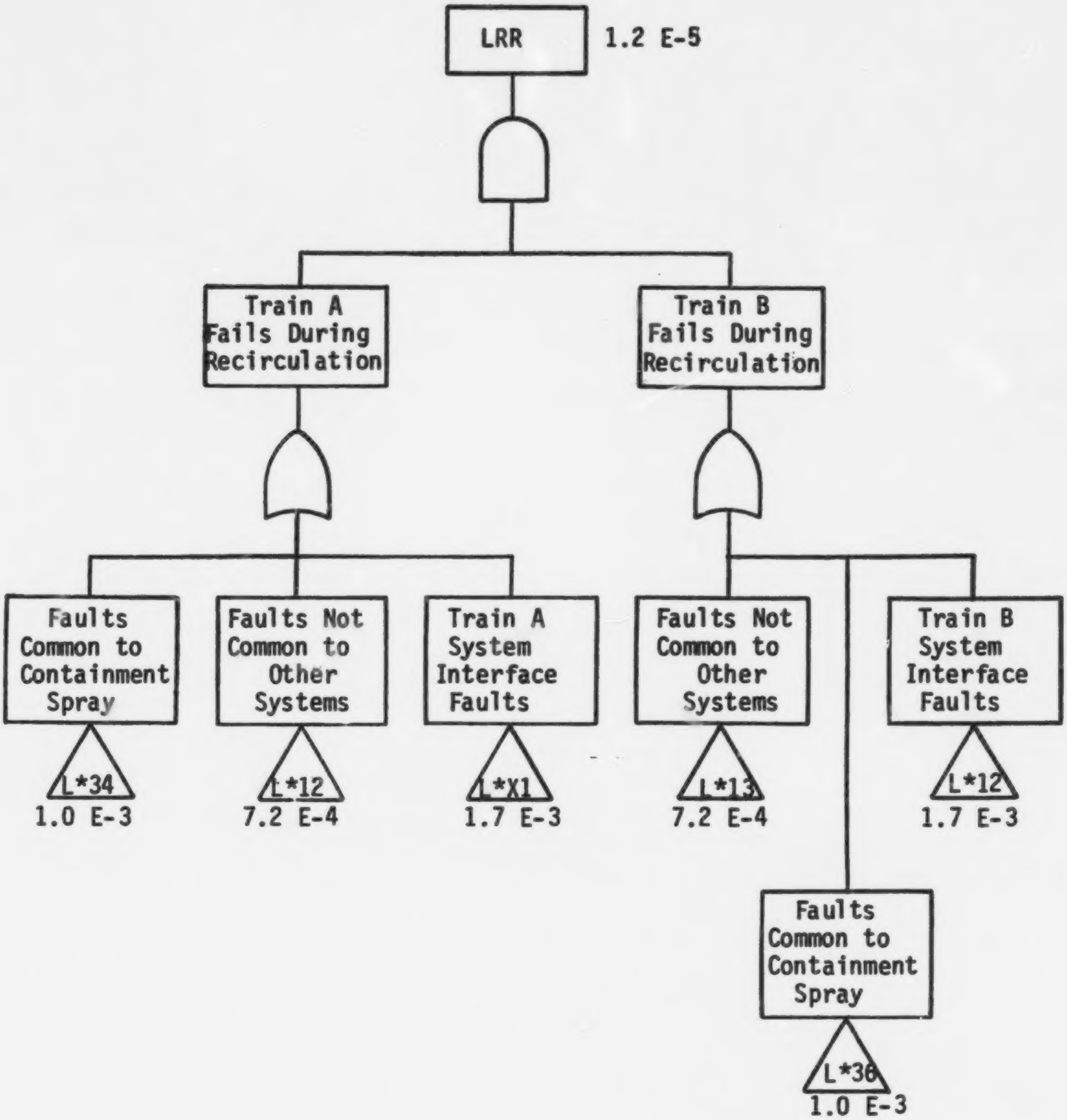

LRR
1.2 E-5
Train A Fails During Recirculation
Train B Fails During Recirculation
Faults Common to Containment Spray
L*34
1.0 E-3
Faults Not Common to Other Systems
L*12
7.2 E-4
Train A System Interface Faults
L*X1
1.7 E-3
Faults Not Common to Other Systems
L*13
7.2 E-4
Train B System Interface Faults
L*12
1.7 E-3
Faults Common to Containment Spray
L*36
1.0 E-3

Figure K.12 Modularized Fault Tree for Event "LRR" (B_1, B_2, B_3 LOCAs)

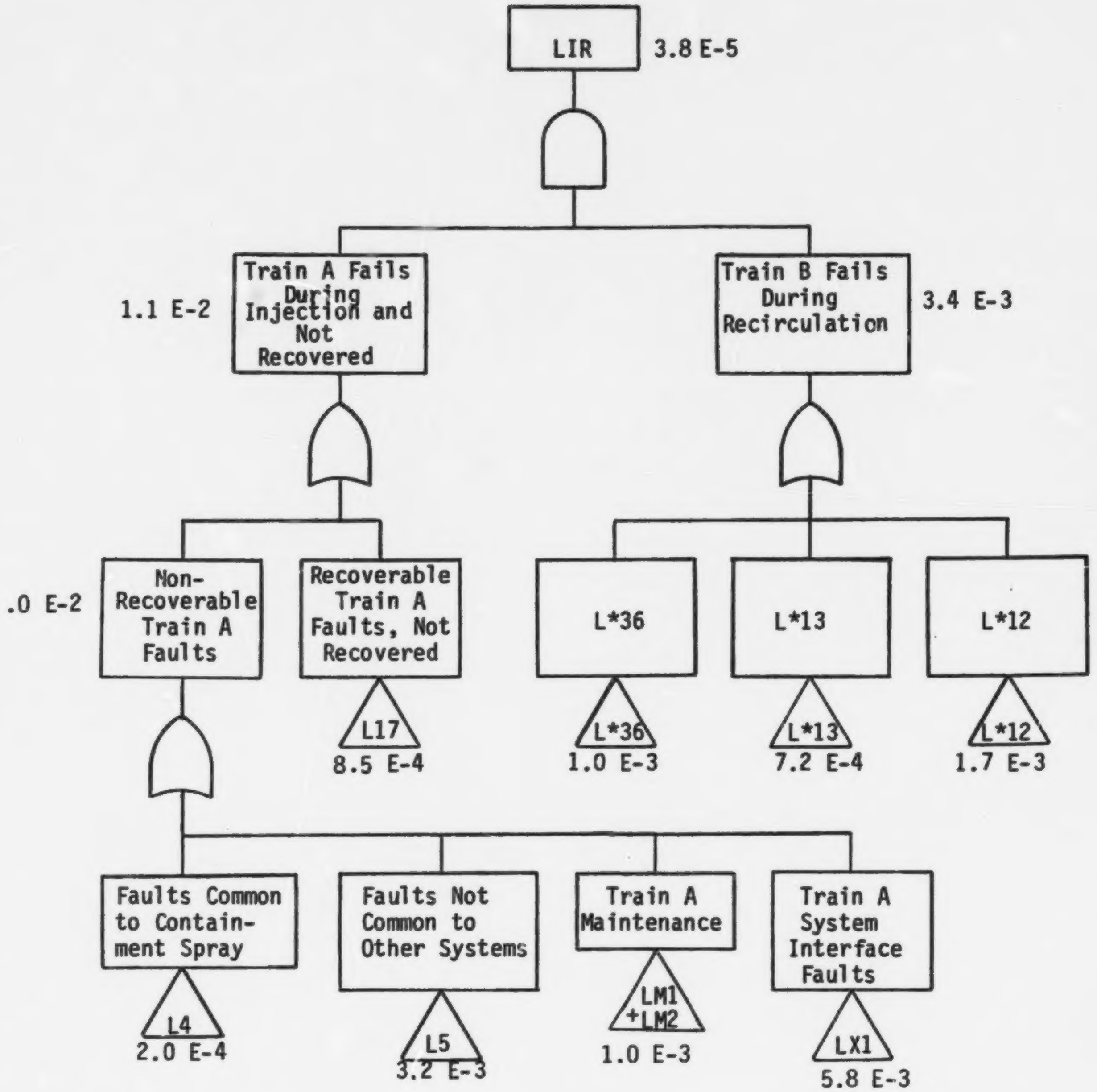

LIR
3.8 E-5
Train A Fails During Injection and Not Recovered
1.1 E-2
Train B Fails During Recirculation
3.4 E-3
.0 E-2
Non-Recoverable Train A Faults
Recoverable Train A Faults, Not Recovered
L17
8.5 E-4
L*36
L*36
1.0 E-3
L*13
L*13
7.2 E-4
L*12
L*12
1.7 E-3
Faults Common to Containment Spray
L4
2.0 E-4
Faults Not Common to Other Systems
L5
3.2 E-3
Train A Maintenance
LM1 +LM2
1.0 E-3
Train A System Interface Faults
LX1
5.8 E-3

Figure K.13 Modularized Fault Tree for Event "LIR" (B_1, B_2, B_3 LOCAs)

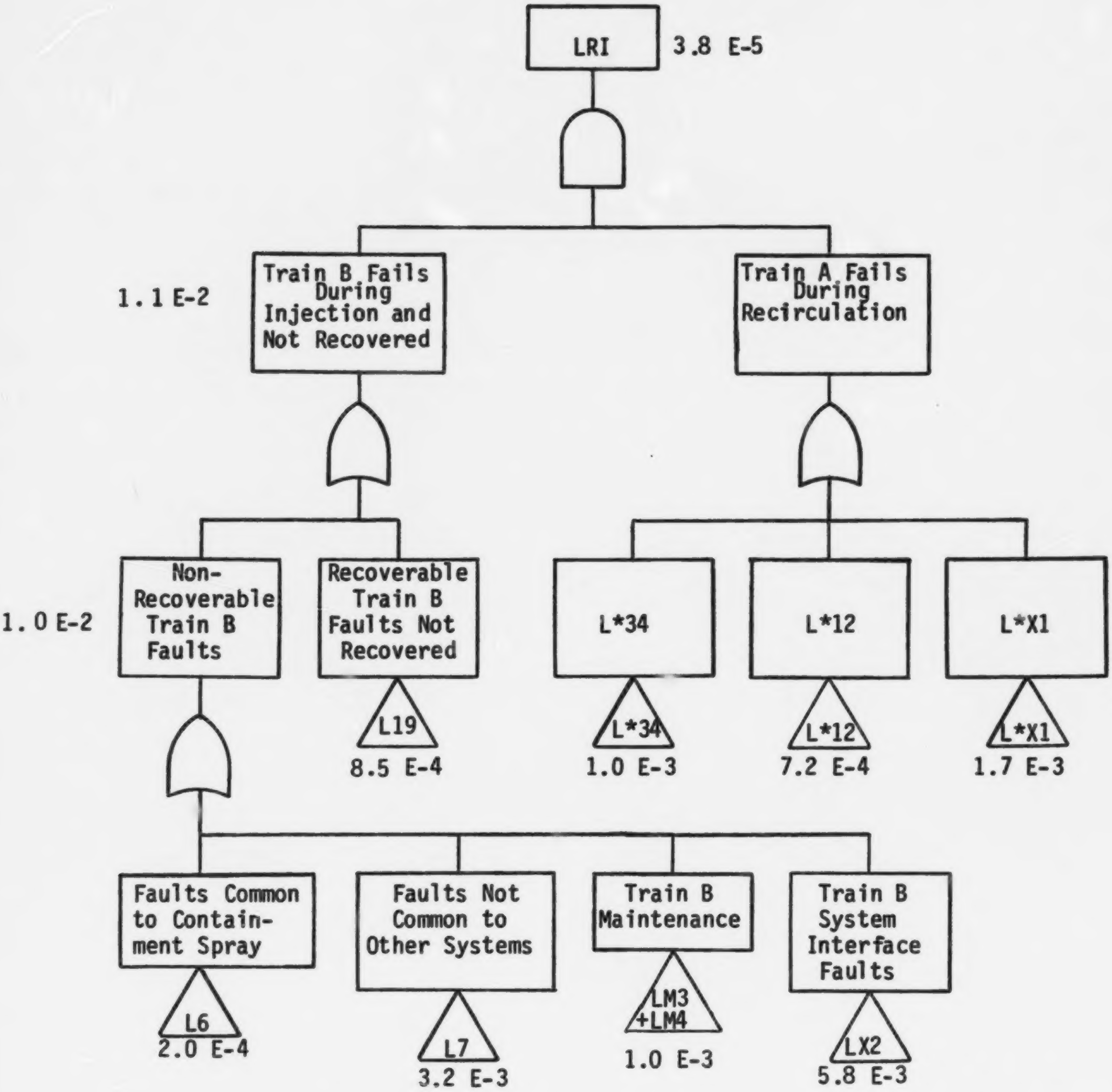

LRI
3.8 E-5
1.1 E-2
Train B Fails During Injection and Not Recovered
Train A Fails During Recirculation
1.0 E-2
Non-Recoverable Train B Faults
Recoverable Train B Faults Not Recovered
L19
8.5 E-4
L*34
L*34
1.0 E-3
L*12
L*12
7.2 E-4
L*X1
L*X1
1.7 E-3
Faults Common to Containment Spray
L6
2.0 E-4
Faults Not Common to Other Systems
L7
3.2 E-3
Train B Maintenance
LM3 +LM4
1.0 E-3
Train B System Interface Faults
LX2
5.8 E-3

Figure K.14 Modularized Fault Tree for EVent "LRI" (B_1, B_2, B_3 LOCAs)

Table K.10 Low Pressure Recirculation (B_4-LOCA)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS | | NOTES

$$LHR = L04 + L06 + L010 + I1 \cdot L09 + (L*34 + LA* + DA) \cdot (L*36 + LB* + DB) \qquad (1)$$

$$\begin{aligned} LHA &= LM2 + L06 + L010 + L04 + I1 \cdot L09 + (L*34 + LA* + DA) \cdot \\ &\quad \cdot (L*36 + LB* + DB + L03) \\ &= LHR + LM2 + L03 \cdot (L*34 + LA* + DA) \qquad (1) \end{aligned}$$

$$\begin{aligned} LHB &= LM4 + L06 + L010 + L04 + I1 \cdot L09 + (L*36 + LB* + DB) \cdot \\ &\quad \cdot (L*34 + LA* + DA + L03) \\ &= LHR + LM4 + L03 \cdot (L*36 + LB* + DB) \qquad (1) \end{aligned}$$

INTERMEDIATE EVENTS

$$\begin{aligned} LA* &= L4 + LM1 + LM2 + LT1 \cdot L011 + L14 + L*X1 \\ LB* &= L6 + LM3 + LM4 + LT2 \cdot L012 + L15 + L*X2 \\ L*X1 &= ACA* + DCA* + DA* \\ L*X2 &= ACB* + DCB* + DB* \end{aligned}$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENT

$$\begin{aligned} LHR = {} & L04 + L06 + L010 + I1 \cdot L09 + (L4 \cdot L6) + (L14 \cdot L15) + \\ & + (DA \cdot DB) + D*1 \cdot D*2 + L6 \cdot L*34 + L4 \cdot L*36 + L*34 \cdot L*36 + \\ & + DA \cdot (L*36 + L6 + LM3 + LM4 + LT2 \cdot L012 + L15 + D*2) + \\ & + DB \cdot (L*34 + L4 + LM1 + LM2 + LT1 \cdot L011 + L14 + D*1) + \\ & + D*1 \cdot (L*36 + L6 + LM3 + LM4 + LT2 \cdot L012 + L15) + \\ & + D*2 \cdot (L*34 + L4 + LM1 + LM2 + LT1 \cdot L011 + L14) + \\ & + L14 \cdot (L*36 + L6 + LM3 + LM4 + LT2 \cdot L012) + \\ & + L15 \cdot (L*34 + L4 + LM1 + LM2 + LT1 \cdot L011) + \\ & + (L*34 + L4) \cdot (LM3 + LM4 + LT2 \cdot L012) + \\ & + (L*36 + L6) \cdot (LM1 + LM2 + LT1 \cdot L011) \qquad (2,3) \end{aligned}$$

Table K.10 Low Pressure Recirculation (B_4-LOCA)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

NOTES

1 These equations are not fully reduced since LM2 appears in LA* and LM4 appears in LB*. The term LM2·LM3 represents simultaneous maintenance outages in both legs, and are omitted since they are prohibited by Technical Specifications.

2 Terms representing simultaneous outages in both legs are omitted since they are prohibited by Technical Specifications.

3 For quantification, events L4·L6 and L14·L15 are assumed to be coupled. (See Fault Tree Quantification Tables.)

Table K.11 Low Pressure Recirculation (B_1, B_2, B_3-LOCAs)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

$$LPR = L04 + L010 + LRR + LIR + LRI$$

$$\begin{aligned}
LRR &= (L^{*}12 + L^{*}34 + L^{*}X1)\cdot(L^{*}36 + L^{*}13 + L^{*}X2) \\
LIR &= (L^{*}13 + L^{*}36 + L^{*}X2)\cdot(L4 + L5 + L17 + LM1 + LM2 + LX1) \\
LRI &= (L^{*}12 + L^{*}34 + L^{*}X1)\cdot(L6 + L7 + L19 + LM3 + LM4 + LX2)
\end{aligned}$$

INTERMEDIATE EVENTS

$$\begin{aligned}
LX1 &= ACA + DCA + DA \\
LX2 &= ACB + DCB + DB
\end{aligned}$$

$$\begin{aligned}
L^{*}X1 &= ACA^{*} + DCA^{*} + DA^{*} \\
L^{*}X2 &= ACB^{*} + DCB^{*} + DB^{*}
\end{aligned}$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENTS

$$\begin{aligned}
LPR &= L04 + L010 + LRR + LIR + LRI \\
LRR &= (ACA^{*}\cdot ACB^{*}) + (DA^{*}\cdot DB^{*}) + ACA^{*}\cdot DB^{*} + ACB^{*}\cdot DA^{*} + \\
&\quad + (L^{*}13 + L^{*}36)\cdot(ACA^{*} + DA^{*}) + (L^{*}12 + L^{*}34)\cdot(ACB^{*} + DB^{*}) + \\
&\quad (L^{*}12 + L^{*}34)\cdot(L^{*}13 + L^{*}36)
\end{aligned}$$

$$\begin{aligned}
LIR &= (ACB^{*} + DB^{*})\cdot(ACA + DA) + \\
&\quad + (LM1 + LM2)\cdot(L^{*}13 + L^{*}36 + ACB^{*} + DB^{*}) \\
&\quad + (L4 + L5 + L17)\cdot(L^{*}13 + L^{*}36 + ACB^{*} + DB^{*}) + \\
&\quad + (ACA + DA)\cdot(L^{*}13 + L^{*}36)
\end{aligned}$$

$$\begin{aligned}
&= (ACA^{*} + DA^{*})\cdot(ACB + DB) + \\
&\quad + (LM3 + LM4)\cdot(L^{*}12 + L^{*}34 + ACA^{*} + DA^{*}) + \\
&\quad + (L6 + L7 + L19)\cdot(L^{*}12 + L^{*}34 + ACA^{*} + DA^{*}) + \\
&\quad + (ACB + DB)\cdot(L^{*}12 + L^{*}34)
\end{aligned}$$

Table K.12 (1/9) Events "LHA" and "LHB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
LA* LB*		SEE QUANTIFICATION TABLE						
L03	OPERATOR	FAILS TO OPEN VALVES DHV-7 AND DHV-8 TO PROVIDE FLOW FROM LEG B(A) TO HIGH PRESSURE TRAIN A (B), GIVEN FAILURE OF LEG A (B)			0.1	$5^+, 5^-$	0	10
L04	OPERATOR	**FAILS TO RECONFIGURE FOR RECIRCULATION**	D		3.0 E-3	$10^+, 10^-$	0	14
L06	OPERATOR	TURNS LPI OFF AND FAILS TO INITIATE	D		5.0 E-2	$3^+, 10^-$	0	
I1	ESAS(ILB3·ILB3)	FAILS TO ACTUATE BOTH PUMPS			ε			
L09	OPERATOR	FAILS TO MANUALLY INITIATE PUMPS	D		1.0 E-2	$3^+, 10^-$	0	
L010	OPERATOR	INADVERTENTLY TERMINATES LOW PRESSURE RECIRCULATION	D		1.0 E-3	$10^+, 10^-$	0	15
LM2	DHV-110	MAINTENANCE OUTAGE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	11
LM4	DHV-111	MAINTENANCE OUTAGE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	11
L*34		FAULTS IN LEG A RECIRCULATION LINE			1.0 E-3			
	DHV-42	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	DHV-42 SWITCH	FAILS TO TRANSFER	D		1.0 E-5	$3^+, 3^-$		
	DHV-42	PLUGGED	3.0 E-7	24	7.2 E-6	$3^+, 3^-$		
					Σ=1.0 E-3			
L*36		FAULTS IN LEG B RECIRCULATION LINE			1.0 E-3			
	DHV-43	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	DHV-43 SWITCH	FAILS TO TRANSFER	D		1.0 E-5	$3^+, 3^-$		
	DHV-43	PLUGGED	3.0 E-7	24	7.2 E-6	$3^+, 3^-$		
					Σ=1.0 E-3			
L4· L6		EVENT INCLUDING COUPLED VALVE FAILURES DHV-34 AND DHV-35			1.0 E-5	$2^+, 2^-$	B	12
L14 L15		EVENT INCLUDING COUPLED PUMP FAILURES DHP-1A AND DHP-1B			1.0 E-4	$2^+, 2^-$	B	13
DA	DHCCCS A TRAIN	INSUFFICIENT COOLING			5.8 E-3			
DB	DHCCCS B TRAIN	INSUFFICIENT COOLING			5.8 E-3			
DA·DB	DHCCCS A&B TRAINS	INSUFFICIENT COOLING			1.4 E-4			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table K.12 (2/9) Events "LA*" Quantification (See Note 1)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L4		FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
	MOV DHV-34	VALVE PLUGGED	D		1.0 E-4	$3^+, 3^-$		17
	DHV-33	CHECK VALVE FAILS TO OPEN (PLUGGED)	D		1.0 E-4	$3^+, 3^-$		17
					Σ=2.0 E-4			
L14		FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION			3.7 E-3			
	DHP-1A	PUMP FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	DHP-1A	PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5	24	7.2 E-4	$10^+, 10^-$		
	CIRCUIT BKR DHP-1A	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	DHV-21	MANUAL VALVE LEFT CLOSED	D		1.0 E-3		H	3
	DPDP-5A FUSE 10	OPEN AND FAILURE TO RECOVER	(0.1)(1.E-6)	168	1.7 E-5	$3^+, 3^-$		2, 9
					Σ=3.7 E-3			
LM1	DHP-1A	OUT FOR MAINTENANCE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	
LM2	DHV-110	OUT FOR MAINTENANCE	.02/720	18	5.0 E-4	$3^+, 3^-$	M	
LT1·L011		LEG A IN TEST AND FAILURE TO RECOVER			8.3 E-4	$3^+, 3^-$	H	
LT1		LEG A IN TEST	2/720	3	8.3 E-3			4
L011		OPERATOR FAILS TO RECOVER FROM TEST BY CLOSING DHV-8 AND DHV-9			0.1	$3^+, 3^-$		5
					π=8.3 E-4			
L*X1		TRAIN A SYSTEM INTERFACE FAULT			1.7 E-3			
ACA*	AC TRAIN A	INSUFFICIENT POWER			ε			6, 7
DCA*	DC TRAIN A	INSUFFICIENT POWER			ε			8
DA*	DHCCCS A TRAIN	INSUFFICIENT COOLING			1.7 E-3			

Table K.12 (3/9) Event "LB*" Quantification (See Note 1)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L6		FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
	DHV-35	VALVE PLUGGED	D		1.0 E-4	3^+, 3^-		17
	CHECK VALVE DHV-36	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		17
					Σ=2.0 E-4			
L15		HARDWARE FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION			3.7 E-3			
	DHP-1B	PUMP FAILS TO START	D		1.0 E-3	3^+, 3^-		
	DHP-1B	PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5	24	7.2 E-4	10^+, 10^-		
	DHP-1B CIRCUIT BREAKER	FAILS TO CLOSE	D		1.0 E-3			
	DHV-32	MANUAL VALVE LEFT CLOSED	D		1.0 E-3		H	3
	DPDP-5B FUSE 10	FAILS OPEN	1.0 E-6	168	1.7 E-4	3^+, 3^-		2
	OPERATOR	FAILS TO RECOVER			0.1			
					π=1.7 E-3			
					Σ=3.7 E-3			
LM3	DHP-1B	OUT OF SERVICE	.02/720	18	5.0 E-4	3^+, 3^-	M	
LM4	DHV-111	OUT OF SERVICE	.02/720	18	5.0 E-4	3^+, 3^-	M	
LT2·LO12		LEG B IN TEST AND FAILURE TO RECOVER			8.3 E-4	5^+, 3^-	H	
LT2		LEB B IN TEST	2/720	3	8.3 E-3			4
LO12		OPERATOR FAILS TO RECOVER FROM TEST BY CLOSING DHV-7 OR DHV-9			0.1	3^+, 3^-		5
					π=8.3 E-4			
L*X2		INTERFACING SYSTEM FAULTS			1.7 E-3			
ACB*		AC TRAIN B INSUFFICIENT POWER			ε			6, 7
DCB*		DC TRAIN B INSUFFICIENT POWER			ε			8
DB*		DHCCCS-B INSUFFICIENT COOLING			1.7 E-3			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table K.12 (4/9) Event "LPR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L04	OPERATOR	FAILS TO RECONFIGURE FOR RECIRCULATION	D		3.0 E-3	10^+, 10^-	0	14
L010	OPERATOR	INADVERTENTLY TERMINATES LOW PRESSURE RECIRCULATION	D		1.0 E-3	10^+,10^-	0	15

Table K.12 (5/9) Event "LRR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L*12		SINGLE HARDWARE FAULTS THAT ARE NOT COMMON TO OTHER SYSTEMS (TRAIN A)			7.2 E-4			
	PUMP DHP-1A	FAILS TO CONTINUE TO RUN	3.0 E-5	24	7.2 E-4			
L*13		SINGLE HARDWARE FAULTS THAT ARE NOT COMMON TO OTHER SYSTEMS (TRAIN B)			7.2 E-4			
	PUMP DHP-1B	FAILS TO CONTINUE TO RUN	3.0 E-5	24	7.2 E-4			
L*34		FAULTS IN TRAIN A COMMON TO CONTAINMENT SPRAY			1.0 E-3			
	MOV DHV-42	NC VALVE FAILS TO OPEN	D		1.0 E-3			
	DHV-42 SWITCH	FAILS TO TRANSFER	D		1.0 E-5			
	DHV-42	PLUGGED	3.0 E-7	24	7.2 E-6			
					Σ=1.0 E-3			
L*36		FAULTS IN TRAIN B COMMON TO CONTAINMENT SPRAY			1.0 E-3			
	MOV DHV-43	NC VALVE FAILS TO OPEN	D		1.0 E-3			
	DHV-43 SWITCH	FAILS TO TRANSFER	D		1.0 E-5			
	DHV-43	PLUGGED	3.0 E-7		7.2 E-6			
					Σ=1.0 E-3			
L*X1		TRAIN A SYSTEM INTERFACE FAULTS			1.7 E-3			
ACA*		AC TRAIN A						
		INSUFFICIENT POWER			ε			
DCA*		DC TRAIN A						
		INSUFFICIENT POWER			ε			
DA*		DHCCCS-A						
		INSUFFICIENT COOLING			1.7 E-3			
L*X2		TRAIN B SYSTEM INTERFACE FAULTS			1.7 E-3			
ACB*		AC TRAIN B						
		INSUFFICIENT POWER			ε			
DCB*		DC TRAIN B						
		INSUFFICIENT POWER			ε			
DB*		DHCCCS-B						
		INSUFFICIENT COOLING			1.7 E-3			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table K.12 (6/9) Event "LIR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L*36		FAULTS IN TRAIN B COMMON TO CONTAINMENT SPRAY (SEE LRR TABLE)			1.0 E-3			
L*13		SINGLE HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LRR TABLE)			7.2 E-4			
L*X2		TRAIN B SYSTEM INTERFACE FAULTS (SEE LRR TABLE)			1.7 E-3			
L4		FAULTS COMMON TO CONTAINMENT SPRAY (SEE LA TABLE)			2.0 E-4			
L5		FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LA TABLE)			3.2 E-3	3^+, 3^-	H	
LM1		DHP-1A OUT FOR MAINTENANCE (SEE LA TABLE)			5.0 E-4	3^+, 3^-	M	
LM2		DHV-110 OUT FOR MAINTENANCE (SEE LA TABLE)			5.0 E-4	3^+, 3^-	M	
LX1		SYSTEM INTERFACE FAULTS: ONLY DHCCCS TRAIN A, NON LOSP (SEE LA TABLE)			5.8 E-3			16
L17		RECOVERABLE TRAIN A FAULTS NOT RECOVERED			8.5 E-4	3^+, 3^-	0	
I2·L013		DHV-5 DOES NOT RECEIVE ESAS AND OPERATOR DOES NOT RECOVER			ϵ			
I2		DHV-5 DOES NOT RECEIVE ESFAS (ILB3)	D		ϵ			
L013		OPERATOR FAILS TO RECOVER			0.1 $\pi=\epsilon$	3^+, 3^-	0	
LT1·L014		LEG A IN TEST AND OPERATOR DOES NOT RECOVER			8.3 E-4			
LT1		LEG A IN TEST		3	8.3 E-3			
L014		OPERATOR FAILS TO RECOVER			0.1 $\pi=8.3$ E-4	3^+, 3^-	0	
I1·L015		DHP-1A DOES NOT RECEIVE ESFAS			ϵ			
I1		PUMP DHP-1A DOES NOT RECEIVE ESFAS (ILB3)	D		ϵ			
L015		OPERATOR FAILS TO RECOVER			0.1 $\pi=\epsilon$	3^+, 3^-	0	

Table K.12 (7/9) Event "LIR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L21·L016		NO POWER FROM DPDP-5A FUSE 10 AND OPERATOR DOES NOT RECOVER			1.7 E-5			
L21		NO POWER FROM DPDP-5A FUSE 10 BLOWN	1.0 E-6	168	1.7 E-4			
L016		OPERATOR DOES NOT RECOVER	D		0.1	3^+, 3^-	0	
					π=1.7 E-5			
					Σ=8.5 E-4			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table K.12 (8/9) Event "LRI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L*34		FAULTS IN TRAIN A COMMON TO CONTAINMENT SPRAY (SEE LRR TABLE)			1.0 E-3			
L*12		TRAIN A FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LRR TABLE)			7.2 E-4			
L*X1		TRAIN A SYSTEM INTERFACE FAULTS (SEE LRR TABLE)			1.7 E-3			
L6		FAULT COMMON TO CONTAINMENT SPRAY (SEE LB TABLE)			2.0 E-4			
L7		FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LB TABLE)			3.2 E-3	3^+, 3^-	H	
LM3		DHP-1B OUT FOR MAINTENANCE (SEE LB TABLE)			5.0 E-4	3^+, 3^-	M	
LM4		DHV-111 OUT FOR MAINTENANCE (SEE LB TABLE)			5.0 E-4	3^+, 3^-	M	
LX2		SYSTEM INTERFACE FAULTS: DB, NON LOSP ONLY (SEE LB TABLE)			5.8 E-3			16
L19		RECOVERABLE TRAIN B FAULTS NOT RECOVERED			8.5 E-4	3^+, 3^-	0	
I2· L013		DHV-6 DOES NOT RECEIVE ESFAS AND OPERATOR DOES NOT RECOVER			ϵ			
I2		DHV-6 DOES NOT RECEIVE ESFAS (ILB3)	D		ϵ			
L013		OPERATOR FAILS TO RECOVER			0.1 $\pi=\epsilon$	3^+, 3^-	0	
LT2· L014		LEB B IN TEST AND OPERATOR DOES NOT RECOVER			8.9 E-4			
LT2		LEG B IN TEST		3	8.9 E-3			
L014		OPERATOR FAILS TO RECOVER			0.1 π=8.9 E-4	3^+, 3^-	0	
I1· L015		DHP-1B DOES NOT RECEIVE ESFAS			ϵ			
I1		PUMP DHP-1B DOES NOT RECEIVE ESFAS (ILB3)	D		ϵ			
L015		OPERATOR FAILS TO RECOVER			0.1 $\pi=\epsilon$	3^+, 3^-	0	

Table K.12 (9/9) Event "LRI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L23· L016		NO POWER FROM DPDP-5B FUSE 10 AND OPERATOR DOES NOT RECOVER			1.7 E-5			
L23		NO POWER FROM DPDP-5B FUSE 10 BLOWN	D		1.7 E-4			
L016		OPERATOR DOES NOT RECOVER			0.1	3^+, 3^-	0	
					π=1.7 E-5			
					Σ=8.9 E-4			

BEST DOCUMENT AVAILABLE

Table K.12 (1/2) Fault Tree Quantification Tables

NOTES

1 Only faults upstream of crossover contribute to LA* or LB*.

2 Fault duration time is 1/2 of 2 weeks, since fuse is tested bi-weekly via pump tests.

3 This fault represents the human error of leaving the valve closed following pump maintenance. The unavailability is estimated as follows: (0.22 maintenance acts per month) X (1.0 E-2 per act) X (360/720 months fault duration).

4 Each leg is operated for about 3 hours every two weeks to recirculate BWST water.

5 The probability of 0.1 is assumed. Recovery involves closing manual valves, but several hours or more would be available before the system is required.

6 See appropriate fault tree analysis.

7 For loss of offsite power transients, this fault is assumed to be recovered, even if the diesel fails, by the time the system is required.

8 DA* includes all faults in DA except failure of the diesel in the case of loss of offsite power transients. Similarly for DB*.

9 The probability of 0.1 is assumed. Recovery involves identifying the open fuse and replacing it, but several hours or more would be available before the system is required.

10 This fault involves failure to provide an alternative flow path by reconfiguring valves DHV-7 and DHV-8. Procedures do not require this operation, but it is an obvious alternative and sufficient time is available to perform the act.

11 LM2 also appears in LA*; LM4 also appears in LB*. The indicated valve is isolated when it is out of service for maintenance, and it is conservatively assumed that the valve bonnet has been removed. Under these conditions, neither leg could provide adequate flow, even if the crossover valves were open.

Table K.12 (2/2) Fault Tree Quantification Tables

NOTES

12 The event L4·L6 was evaluated assuming coupled failures between valves DHV-34 and DHV-35. A coupling coefficient (conditional probability of failure of both valves, given failure of one valve, or β factor) of 0.1 was assumed.

13 The event L14·L15 was evaluated assuming coupled failures between pumps DHP-1A and DHP-1B. A coupling coefficient (conditional probability of failure of both pumps, given failure of one pump or β factor) of 0.1 was assumed.

14 This fault might occur in several different ways:

(a) The operator fails to open the recirculation valves DHV-42 and DHV-43.
(b) Operator opens recirculation valves, but fails to close the injection line suction valves DHV-34 and DHV-35 (this may not fail the system).
(c) Operator closes the injection line valves before opening the recirculation valves, and the time between these acts is sufficiently large to fail the pumps.

15 This fault was included since the operator is required by procedure to terminate operation of the low pressure pumps when they are activated by ESFAS during the injection phase.

16 For the events LX1 and LX2, the non loss of the offsite power numbers for DHCCCS Trains A and B are used, since it is assumed that offsite power is restored by the recirculation phase.

17 It is assumed that if the suction line from the BWST is plugged (or the MOV closed) when the LP pump is turned on, it will cavitate and eventually fail. This fault may occur when the pump is automatically actuated by an ESAS signal or when the operator starts the pump prior to reconfiguring the suction lineup to the sump for LPR.

Table K.13 (1/2) Low Pressure Recirculation - Quantification Summary (B_4 LOCA)

BOOLEAN VARIABLE	POINT ESTIMATES
L4	2.0 E-4
L14	3.7 E-3
LM1	5.0 E-4
LM2	5.0 E-4
LT1·LO11	8.3 E-4
LT1	8.3 E-3
LO11	0.1
L*X1	1.7 E-3
ACA*	ε
DCA*	ε
DA*	1.7 E-3
L6	2.0 E-4
LM3	5.0 E-4
LM4	5.0 E-4
LT2·LO12	8.3 E-4
LT2	8.3 E-3
LO12	0.1
L15	3.7 E-3
L*X2	1.7 E-3
ACB*	ε
DCB*	ε
DB*	1.7 E-3
LA*	7.7 E-3
LB*	7.7 E-3
LO3	0.1
LO4	3.0 E-3

Table K.13 (2/2) Low Pressure Recirculation - Quantification Summary (B_4 LOCA)

BOOLEAN VARIABLE	POINT ESTIMATES
L06	5.0 E-2
I1	ε
L09	1.0 E-2
L010	1.0 E-3
LM2	5.0 E-4
LM4	5.0 E-4
L*34	1.0 E-3
L*36	1.0 E-3
L4·L6	1.0 E-5
L14·L15	1.0 E-4
L17	8.5 E-4
L19	8.5 E-4

[redacted]

Table K.14 Low Pressure Recirculation - Quantification Summary (B_1, B_2, B_3 LOCAs)

BOOLEAN VARIABLE	POINT ESTIMATES
L04	3.0 E-3
L010	1.0 E-3
L*12	7.2 E-4
L*13	7.2 E-4
L*34	1.0 E-3
L*36	1.0 E-3
L*X1	1.7 E-3
ACA*	ε
DCA*	ε
DA*	1.7 E-3
L*X2	1.7 E-3
ACB*	ε
DCB*	ε
DB*	1.7 E-3
L4	2.0 E-4
L5	3.2 E-3
LM1	5.0 E-4
LM2	5.0 E-4
LX1	5.8 E-3
L17	8.5 E-4
L6	2.0 E-4
L7	3.2 E-3
LM3	5.0 E-4
LM4	5.0 E-4
LX2	5.8 E-3
L19	8.5 E-4

APPENDIX L

REACTOR BUILDING EMERGENCY COOLING SYSTEM (RBECS)[*]

---

[*] The RBECS is the emergency operating mode of the Reactor Building Cooling System (RBCS).

APPENDIX L REACTOR BUILDING EMERGENCY COOLING SYSTEM (RBECS)

L.1 SYSTEM DESCRIPTION AND OPERATION

Two redundant and diverse cooling systems are provided to cool the Reactor Building (RB) atmosphere during post accident time periods. RB cooling is necessary in order to prevent overpressurization and potential subsequent failure. The Reactor Building Emergency Cooling System (RBECS) is the first source of heat removal. The Reactor Building Spray System (RBSS) in conjunction with the Decay Heat Removal System (DHRS) provide a redundant heat removal capability. A simplified schematic is shown in Figure L.1.

The RBECS consists of three fan/cooler assemblies. This system is independent and diverse from the spray system. The RBECS simply circulates containment air through the coolers. During emergency service, the heat load from the fan coolers is diverted to the Nuclear Services Closed Cycle Cooling System (NSCCCS).

L.1.1 SYSTEM DESCRIPTION

The RBECS is comprised of three large fan assemblies. A schematic diagram of the fan system is shown in Figure L.1. Each assembly consists of an air to water heat exchanger, a fan, fan motor, a roughing filter to act as a demister, and associated ducting. The ducting inlets are distributed throughout the upper containment. There is one common ducting system for all three fans. Two of the fans are located at EL 95 (bottom of the reactor building) and the third at EL 119. The air from the lower fans is discharged into the reactor building at EL 102. The air from the upper fan is discharged into the reactor building at EL 135.

Power for the fans is supplied by the 480V ESMCC's, one fan being on each of the 3A, 3B and AB centers. This way, failure of either 480V train will only fail one fan. Each fan has two motor coils, a high speed coil for normal operation and a low speed coil for emergency operation. Two fans operate during normal plant operation. Back pressure dampers in the ducting restrict airflow to the inactive fan assembly.

The cooling water flow to all three cooler assemblies is provided by the industrial cooling system during normal plant operation. During emergency operation the fan cooling water supply is switched to the NSCCCS to accommodate the increased heat load.

The lines to and from the individual coolers penetrate the containment. Each line has a containment isolation valve. Manual block valves are provided on either side of the isolation valves. Differential flow meters are provided on each side of the cooler to detect leaks in the cooler assembly. The differential flow meters are displayed and annunciated in the control room. The fan is the only other instrumented component in the system. Annunciated in the control room are the high speed coil trip, low air flow, and fan assembly vibration. The fan motor bearing temperature is computer alarmed. Major component data are listed in Table L.1.

L.1.2 SYSTEM OPERATION

Cooling water flows through all three coolers continuously, regardless of the status of the fan. The water flow is 530 gpm/air handling unit. The cooling water outlet temperature of 85^{o}F is raised by 8^{o}F. During normal operation the heat load per fan assembly is $2X10^{6}$ BTU/hr. The post-LOCA saturated condition of the containment atmosphere raises the heat load to $80X10^{6}$ BTU/hr per fan assembly. In order to accommodate this emergency heat load, the fan coils are switched over to the NSCCCS. The cooling water flow rate increases to 1700 gpm/assembly, the inlet temperature rises to 105^{o}F. The emergency mode of the fans is activated by the ESAS when the reactor building pressure reaches 4 psig.

The configuration changes necessary on an ESAS are summarized below:

(1) The high speed coil on the fan is de-energized and the low speed coil is energized. This is to compensate for the increased pumping requirements of the fans in the saturated containment atmosphere.

(2) The third fan is activated. During normal operation, only two fans are operating. The third is activated to provide redundancy. Airflow through the inactivated cooler is restricted by a set of back pressure, gravity flow dampers. These are expected to open automatically when the fan starts.

(3) The heat load is switched from the industrial cooler to the NSCCCS. This is necessary because of the larger heat loads in the emergency mode as opposed to the normal mode of operation. The inlet and outlet valves (SWV-354 and 353) are opened to connect the fans to the NSCCCS. Inlet and outlet valves from the industrial cooler (SWV-151, 152, 355) are closed.

No requirement for valve alignment checks exists because the fans are a normally operating system. Each fan is required to be demonstrated operable monthly on a staggered test basis (SP-344). The fan has to be operated for 15 minutes and a coolant flow of 500 gpm must be verified. SWV-353 and 354 are stroked once a quarter. Technical Specification 3.6.2.3 requires that two fans be available for normal plant operation. Normal plant operation with only one fan available is limited to 72 hours.

Table L.1 (1/2) Reactor Building Cooling Unit Performance and Equipment Data

(Capacities are on a per air handling unit basis.)

	Duty	
Performance Data	Emergency	Normal
No. Installed	3	3
Type Coil	Finned Tube	Finned Tube
Design Heat Load, Btu/h	80×10^6	2.15×10^6
Fan Capacity, cfm	54,000	108,000
Reactor Building Atmosphere Inlet Conditions		
Temperature, F	281	110
Steam Partial Pressure, psia	49.99	---
Air Partial Pressure, psia	18.31	---
Total Pressure, psia	68.30	Atmospheric
Cooling Water Flow, gpm	1,780	530
Cooling Water Inlet Temperature, F	105	85
Cooling Water Outlet Temperature, F	183	93.1

Equipment Construction Data

Item	Description
Coil Tubes	5/8 in. OD seamless copper with 0.049 in. wall
Coil Fins	0.008 in. thick copper spaced 8.5 per inch
Coil Headers	Schedule 40 steel pipe
Plenum Casing	1/4 in. steel plate
Fan Casing	1/4 in. steel plate
Motor	Pipe ventilated--air to water heat exchanger
Casing Material	ASTM A-36

Table L.1 (2/2) Reactor Building Cooling Unit Performance and Equipment Data

(Capacities are on a per air handling unit basis.)

Summary of Requirements for
Reactor Building Fan Cooling Units

Item	Acceptance Standard
Cooling Coils	
Tubes and Fins	ASTM Material Specification
Hydrostatic Test	ASME Section VIII
Demisters	ASTM Material Specification
Casing and Miscellaneous Parts	ASME Material Specification
Painting	SSPCS SP-1063T
Piping	
Fabrication, Welding, and Inspection	USAS B31.1
Seismic Requirements	Seismic Class I
Motors	NEMA MG-1, ANSI C50.2 and 50.20, IEEE

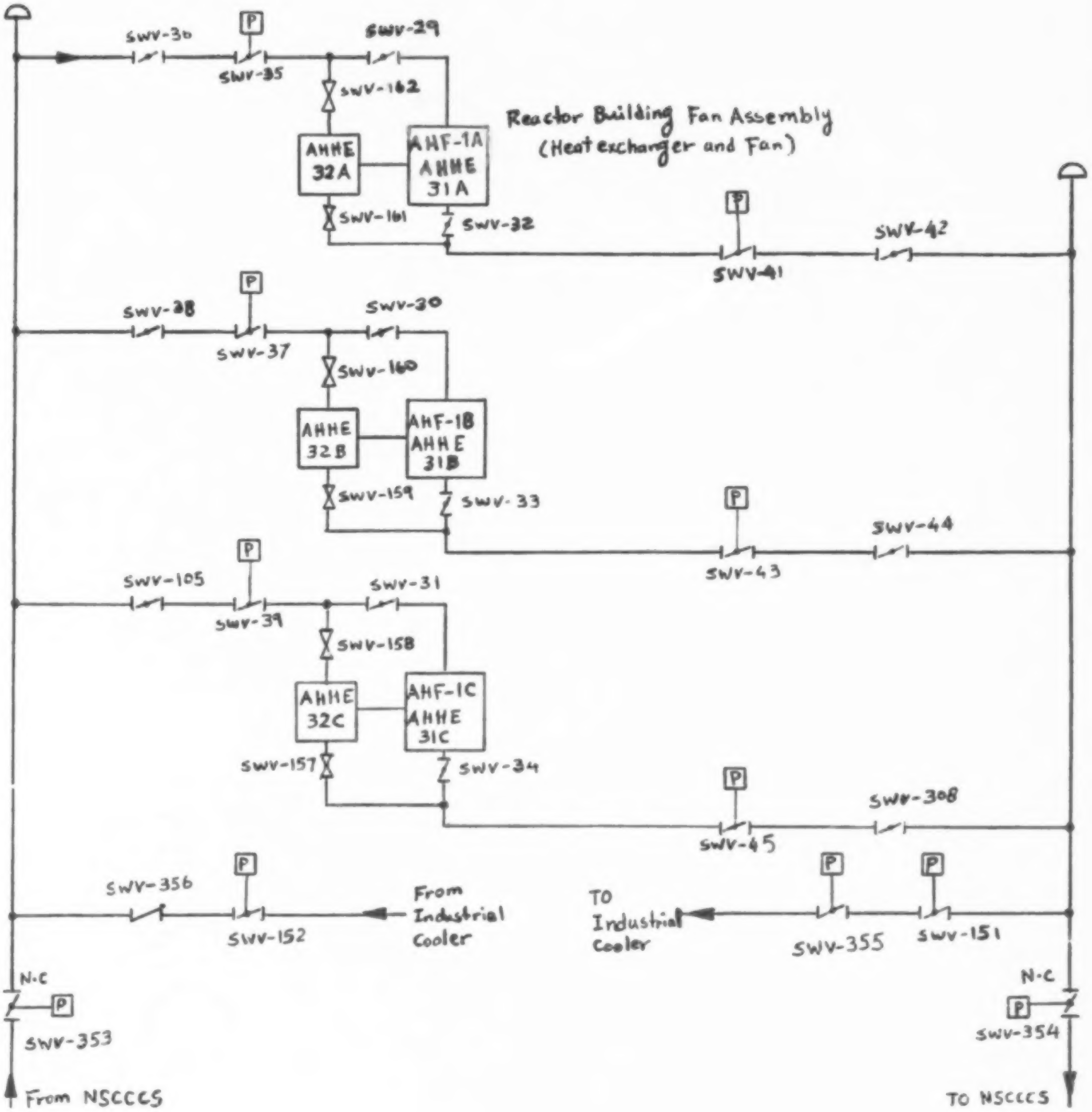

SWV-36
P
SWV-35
SWV-29
SWV-162
AHHE 32A
AHF-1A AHHE 31A
Reactor Building Fan Assembly
(Heat exchanger and Fan)
SWV-161
SWV-32
P
SWV-41
SWV-42
P
SWV-38
SWV-37
SWV-30
SWV-160
AHHE 32B
AHF-1B AHHE 31B
SWV-159
SWV-33
P
SWV-43
SWV-44
P
SWV-105
SWV-39
SWV-31
SWV-158
AHHE 32C
AHF-1C AHHE 31C
SWV-157
SWV-34
P
SWV-45
SWV-308
SWV-356
P
SWV-152
From Industrial Cooler
TO Industrial Cooler
P
SWV-355
P
SWV-151
N.C
P
SWV-353
From NSCCCS
N.C
P
SWV-354
TO NSCCCS

Figure L.1 Reactor Building Emergency Cooling System Schematic Diagram

L.2 SYSTEM SIMPLIFIED FAULT TREE

The detailed fault tree, initially drawn for the RBECS, was simplified in a series of intermediate steps. The simplified fault tree is shown in Figure L.2.

The top event for the fault tree is defined as:

Failure of all fans - failure of at least one fan cooler to operate at rated emergency conditions.

MAJOR ASSUMPTIONS

The major assumptions used to construct the detailed fault tree are listed below:

1. Technical Specification 3.6.2.3 allows operation with only one operable fan for 72 hours. This situation is accounted for in the fault tree.
2. The fans are normally operating and can therefore be expected to have the correct valve alignment at ESAS initiation. However, since one fan is inactive during normal plant operation, there is a possibility it will not have correct valve alignment. Each assembly is required (T.S. 4.6.2.3) to be tested and flow verified, once a month. Each cooler is flow monitored in the control room. Valve mispositions were only listed for the inactive cooler assembly.
3. If the high speed coil is not de-energized, the fan motor will overheat and burn out.
4. Missile damage was assumed possible to the ducting and piping which would fail the fan cooling system, although unlikely.
5. SWV-353 and SWV-354 are stroked once a month, per SP-351.
6. The fan motors and bearings are self-cooled.
7. Airflow across the inactive cooler is zero. Full NSCCCS flow continues through the cooler. Back-pressure gravity dampers starve the airflow. They should open when the fan motor starts.

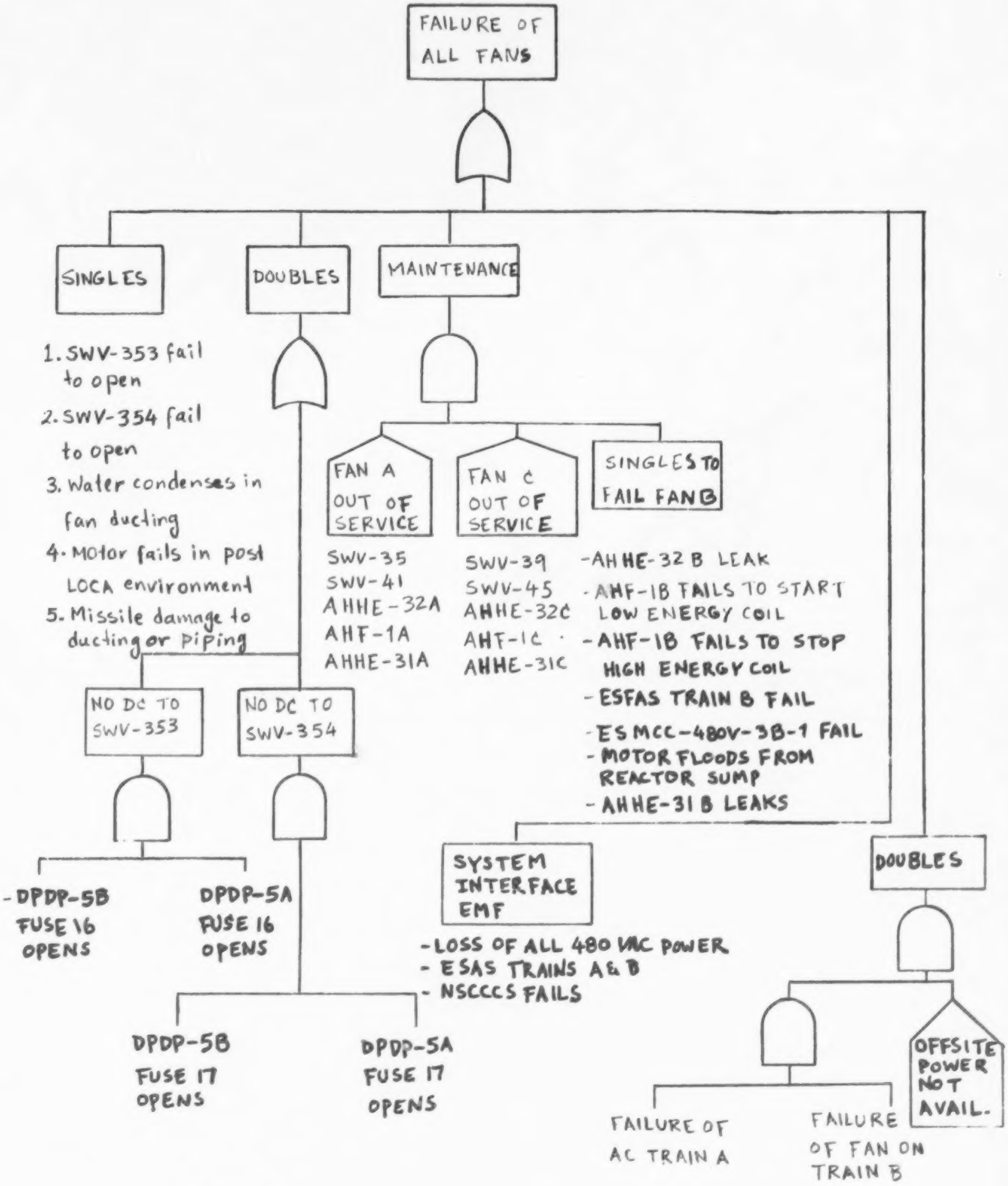

FAILURE OF ALL FANS
SINGLES
DOUBLES
MAINTENANCE
1. SWV-353 fail to open
2. SWV-354 fail to open
3. Water condenses in fan ducting
4. Motor fails in post LOCA environment
5. Missile damage to ducting or piping
FAN A OUT OF SERVICE
FAN C OUT OF SERVICE
SINGLES TO FAIL FAN B
SWV-35
SWV-41
AHHE-32A
AHF-1A
AHHE-31A
SWV-39
SWV-45
AHHE-32C
AHF-1C
AHHE-31C
-AHHE-32B LEAK
-AHF-1B FAILS TO START LOW ENERGY COIL
-AHF-1B FAILS TO STOP HIGH ENERGY COIL
-ESFAS TRAIN B FAIL
-ESMCC-480V-3B-1 FAIL
-MOTOR FLOODS FROM REACTOR SUMP
-AHHE-31B LEAKS
NO DC TO SWV-353
NO DC TO SWV-354
-DPDP-5B FUSE 16 OPENS
DPDP-5A FUSE 16 OPENS
DPDP-5B FUSE 17 OPENS
DPDP-5A FUSE 17 OPENS
SYSTEM INTERFACE EMF
-LOSS OF ALL 480 VAC POWER
-ESAS TRAINS A & B
-NSCCCS FAILS
DOUBLES
OFFSITE POWER NOT AVAIL.
FAILURE OF AC TRAIN A
FAILURE OF FAN ON TRAIN B

Figure L.2 Simplified Fault Tree - RBECS

L.3 SYSTEM QUANTIFICATION

L.3.1 SYSTEM RELIABILITY CHARACTERISTICS

For cases where offsite power is available the main contributor to the unavailability of the RBECS during the injection phase is failure to admit cooling to the fans from the NSCCCS. Cooling water from the NSCCCS is admitted to the fan coolers when the air-operated valves SWV-353 and -354 receive an ESAS signal. However, if offsite power is not available the dominant contributor to the system's unavailability is failure of both diesels to start and power from both units CR-1 and -2 is not available (the unavailability of both fossil units was assessed as 0.36).

About a factor of two smaller is the probability that the NSSWS does not remove heat from the NSCCCS. Failure of both seawater pumps (RWP-2A and 2B) to start or failure of the check valves in the pump discharge to open are the main contributors. The remainder of the failures responsible for the unavailability of RBECS are at least one order of magnitude smaller than the above. They are mainly hardware failures in the NSCCCS. The unavailability of the RBECS during the recirculation phase is dominated by the failure of all fans to run. Failure of all fans to run was assessed as a strongly coupled failure since the three fans operate in the same severe post-LOCA containment atmosphere. The unavailability of RBECS is about the same for both post-accident phases.

L.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE*

This section presents the quantification of the RBECS unavailability for emergency operation during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification the simplified fault tree presented in Section L.2 was transformed into a modularized fault tree.

Table L.2 shows the RBECS success requirements. Table L.3 contains the top event definitions for the modularized fault tree. The unavailability of each gate is shown on the tree, Figure L.3. Table L.4 shows the Boolean equations that represent the fault tree. Table L.5 shows the quantification of each gate by component and failure mode. Table L.6 summarizes the point estimates for each gate.

---

*The RBECS is analyzed in terms of its fan cooler availability. Therefore, the RBECS is referred to as "fan coolers" in this and the following section.

Table L.2 Fan Coolers - Injection

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B_1, B_2, B_3, B_4	1/3 fans	

Table L.3 Fan Coolers - Injection

TOP EVENT DEFINITION

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
FCI	Failure of fan cooler system to provide at least 1/3 fan cooling to containment during injection phase.	

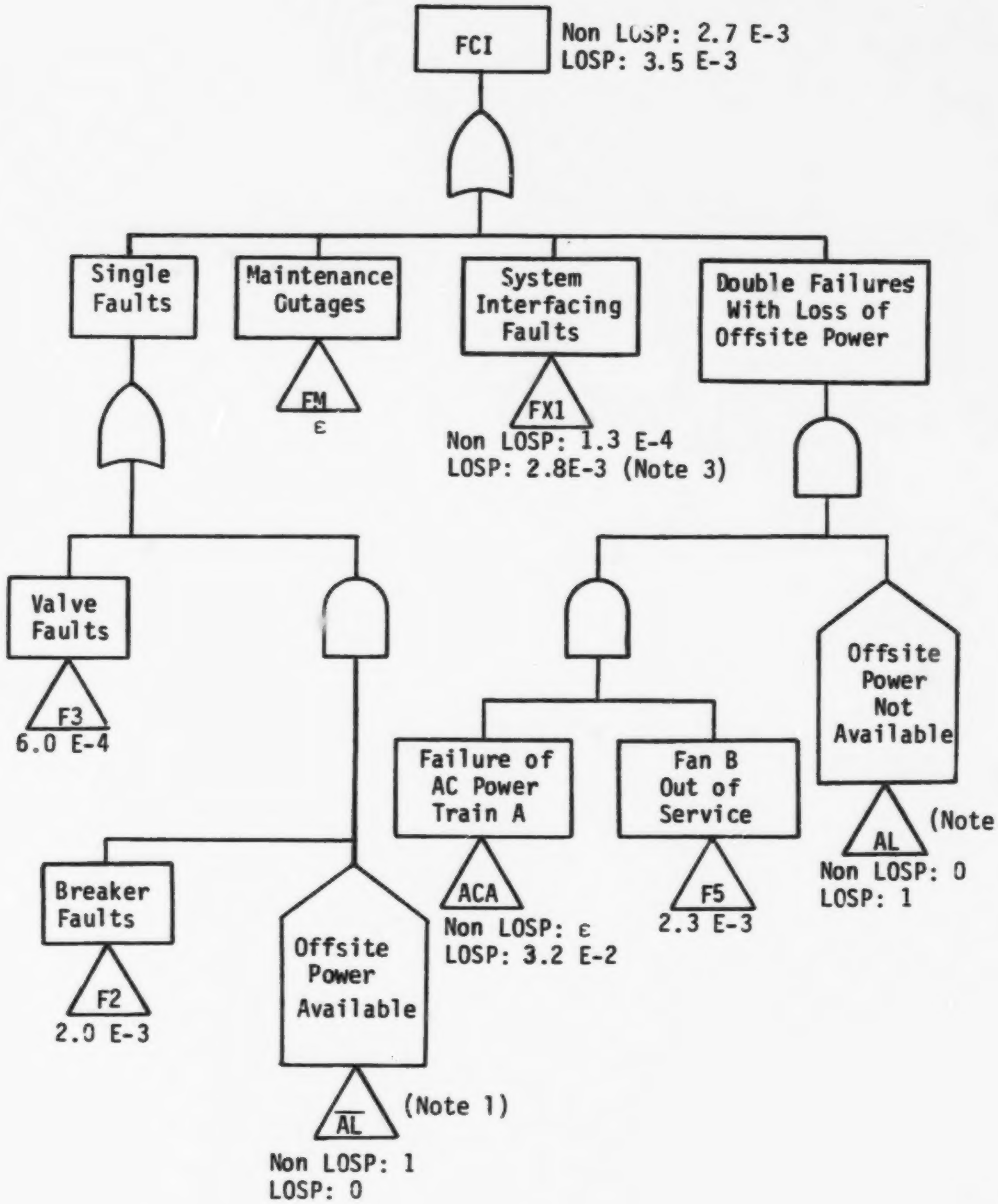

FCI
Non LOSP: 2.7 E-3
LOSP: 3.5 E-3
Single Faults
Maintenance Outages
System Interfacing Faults
Double Failures With Loss of Offsite Power
FM
ε
FX1
Non LOSP: 1.3 E-4
LOSP: 2.8E-3 (Note 3)
Valve Faults
F3
6.0 E-4
Failure of AC Power Train A
Fan B Out of Service
Offsite Power Not Available
ACA
Non LOSP: ε
LOSP: 3.2 E-2
F5
2.3 E-3
AL
(Note
Non LOSP: 0
LOSP: 1
Breaker Faults
F2
2.0 E-3
Offsite Power Available
$\overline{AL}$
(Note 1)
Non LOSP: 1
LOSP: 0

Figure L.3 Modularized Fault Tree for Event "FCI"

Figure L.3 Fan Coolers - Injection

FAULT TREE

NOTES

1 For cases where offsite power is available, house $\overline{AL}$ is one; for cases where offsite power is not available house $\overline{AL}$ is zero.

2 AL is the complement of house $\overline{AL}$. For cases where offsite power is available, house AL is zero; for cases where offsite power is not available house AL is one.

3 This value was obtained from a Boolean reduced form of $N + ACA \cdot ACB + DCA \cdot DCB$.

Table L.4 Fan Coolers - Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT	NOTES
$FCI = \overline{AL} \cdot F2 + F3 + FX1 + AL \cdot ACA \cdot F5 + FM$	(1,2)

BOOLEAN EQUATION WITH TERMS REGROUPED FOR SEQUENCE ANALYSIS

$FCI = F4 + FX1 + AL \cdot ACA \cdot F5$

$F4 = \overline{AL} \cdot F2 + F3 + FM$

$FX1 = N + ACA \cdot ACB + DCA \cdot DCB$

NOTES: 1. Maintenance outage contributions are negligible for this system since it was assumed that only very rarely would 2 fans be out for maintenance.

2. Fans A and C are powered from AC - Train A, while fan B is powered from AC - Train B. Therefore, loss of AC - Train A and fan B out of service is a double failure to FCI. The opposite case involves triple failures and therefore is not shown on the fault tree.

BEST DOCUMENT AVAILABLE

Table L.5 (1/2) Event "FCI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
$\overline{AL}$		HOUSE FOR AVAILABILITY OF OFFSITE POWER			1, 0			1
		NON LOSP			1			
		LOSP			0			
F2		CIRCUIT BREAKER FAULTS			2.0 E-3			
	CIRCUIT BKR SWV-353	FAILS TO TRANSFER	D		1.0 E-3	3^+, 3^-		
	CIRCUIT BKR SWV-354	FAILS TO TRANSFER	D		1.0 E-3	3^+, 3^-		
					Σ=2.0 E-3			
F3		VALVE FAULTS						
	PNEUMATIC VALVE SWV-353	FAILS TO OPEN	D		3.0 E-4	3^+, 3^-		
	PNEUMATIC VALVE SWV-354	FAILS TO OPEN	D		3.0 E-4	3^+, 3^-		
					Σ=6.0 E-4			
FM		MAINTENANCE OUTAGES			ε			2
FX1		SYSTEM INTERFACING FAULTS						
		NON LOSP			1.3 E-4			3
		LOSP			2.8 E-3			
ACA· ACB		AC POWER FAILS						
		NON LOSP			ε			
		LOSP			2.3 E-3			
N		NSCCCS FAILS TO PROVIDE COOLING (SEE QUANTIFICATION TABLES FOR N)						
		NON LOSP			1.3 E-4			
		LOSP			2.8 E-3			
AL		COMPLEMENT OF $\overline{AL}$			0, 1			
		NON LOSP			0			
		LOSP			1			

Table L.5 (2/2) Event "FCI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ACA		AC TRAIN A FAILS						
		NON LOSP			ε			
		LOSP			3.2 E-2			
F5		FAN B OUT OF SERVICE			2.3 E-3			
	FAN AHF-1B	FAILS TO START	D		3.0 E-4	$3^+,3^-$		
	CIRCUIT BKR. AHF-1B(HI)	FAILS TO TRANSFER	D		1.0 E-3	$3^+,3^-$		
	CIRCUIT BKR. AHF-1B(LO)	FAILS TO TRANSFER	D		1.0 E-3	$3^+,3^-$		
					Σ=2.3 E-3			

BEST DOCUMENT AVAILABLE

Table L.5 Fan Coolers - Injection

QUANTIFICATION TABLES

NOTES

1 For offsite power available, house has a value of one; for offsite power not available, house has a value of zero. On loss of offsite power air operated valves configure to open position without requiring breaker operation.

2 Maintenance outages were assumed to not contribute since it was assumed that only rarely would two fans be in maintenance at the same time.

3 After Boolean reduction, FX1 = N.

Table L.6 RBECS - Injection Phase Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
$\bar{A}$L	1* 0**
F2	2.0 E-3
F3	6.0 E-4
FM	ε
AL	0* 1**
F5	2.3 E-3
ACA	ε* 3.2 E-2**
ACA·ACB	ε* 2.3 E-3**

*Offsite power available
**Offsite power not available

L.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the RBECS unavailability for emergency operation during the recirculation phase of a postulated accident. As for the injection phase, a modularized fault tree was constructed.

Table L.7 shows the RBECS success requirements. Table L.8 contains the top event definitions for the modularized tree, and Figure L.4 shows the modularized fault tree. The unavailability of each gate is shown on the tree. Table L.9 shows the Boolean equations that represent the fault tree. Table L.10 shows the quantification of each gate by component and failure mode. Table L.11 summarizes the point estimates for each gate.

Table L.7 Fan Coolers - Recirculation

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B_1, B_2, B_3, B_4	1/3 Fans	

Table L.8 Fan Coolers - Recirculation

TOP EVENT DEFINITION

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
FCR	Failure of fan cooler system to provide at least 1/3 fan cooling to containment during recirculation phase	

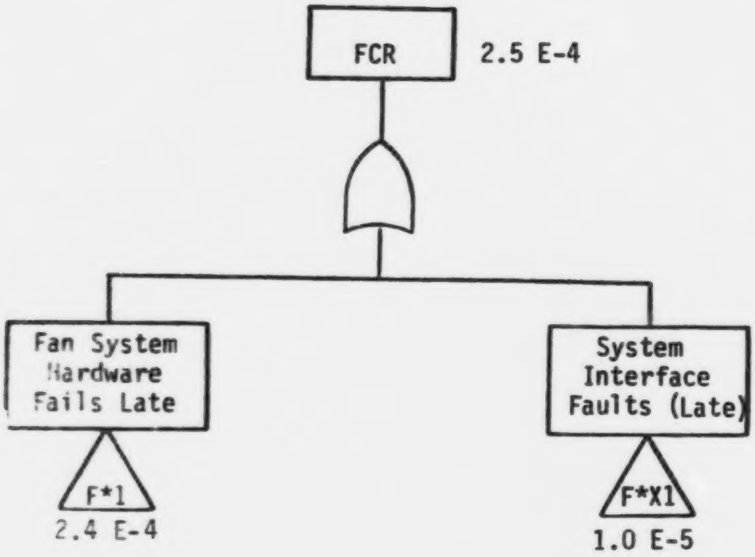

FCR
2.5 E-4
Fan System Hardware Fails Late
F*1
2.4 E-4
System Interface Faults (Late)
F*X1
1.0 E-5

Figure L.4 Modularized Fault Tree for Event "FCR"

Table L.9 Fan Coolers - Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT	NOTES
FCR = F*1 + F*X1	

INTERMEDIATE EVENTS	
F*X1 = N* + ACA*·ACB*	(1)

NOTES: 1. Offsite power is assumed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

BEST DOCUMENT AVAILABLE

Table L.10 Event "FCR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
F*1		FAN SYSTEM HARDWARE FAILS LATE			2.4 E-4			
	3 FANS	FAILS IN POST-LOCA ENVIRIONMENT	(1.0 E-4)(0.1)	24	2.4 E-4	2^+, 2^-	B	1
F*X1		INTERFACING SYSTEM FAULTS						
N*		MSCCCS FAILS DURING RECIRCULATION (SEE QUANTIFICATION TABLE FOR N*)			1.0 E-5			
ACA*· ACB*		AC POWER FAILS DURING RECIRCULATION			ϵ			

Table L.10 Fan Coolers - Recirculation

QUANTIFICATION TABLES

NOTES

1 This fault was assessed assuming that failure of all 3 fans in the post-LOCA environment would be coupled. A failure rate of 1.0 E-4/hr. was used as the basic failure rate (intermediate between the normal and extreme environment failure rates given in WASH-1400).

Table L.11 RBECS - Recirculation Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
F*1	2.4 E-4
ACA*·ACB*	ε

APPENDIX M

REACTOR BUILDING SPRAY SYSTEM (RBSS)

APPENDIX M REACTOR BUILDING SPRAY SYSTEM (RBSS)

M.1 SYSTEM DESCRIPTION AND OPERATION

The Reactor Building Spray System is designed to furnish reactor building atmosphere cooling to reduce the building pressure after LOCA. In addition, the sprays reduce the fission product iodine inventory from the containment atmosphere. The pressure reduction function of the sprays serves as a back-up to the reactor building emergency cooling system (RBECS, Appendix L). The RBSS is an engineered safety feature and performs no normal operating function.

M.1.1 SYSTEM DESCRIPTION

The RBSS, Figure M.1, is a once-through, two train system, taking suction from the low pressure injection system suction header and discharging into the containment atmosphere. Each of the two independent trains is rated at 100% pressure reduction and iodine removal capacity and consists of a pump, a spray header, associated piping, valves, instrumentation, and controls.

The spray pumps are powered from 4160V ES busses. Cooling to pump BSP-1A and BSP-1B is provided by Trains A and B, respectively, of the Decay Heat Closed Cycle Cooling System (DHCCCS, see Appendix F). The water source for the sprays during the injection phase is the BWST and during the recirculation phase the reactor building sump. The low pressure injection and recirculation system suction header configuration is described in Appendix K. Old connections for addition of sodium thio-sulfate to the spray water exist between check valve BSV-1 and spray pump BSP-1A in Train A and between BSV-8 and BSP-1B in Train B (see Figure M.1). However, the sodium thio-sulfate admission valves BSV-99 and 100 are locked closed (according to procedure OP-405) and the tanks are drained.

Each spray pump can discharge 1500 gpm at the rated head of 450 ft into the containment atmosphere through spray nozzles. There are 192 nozzles located on nine spray rings, evenly divided between both spray trains (4 spray rings for Train A, 5 spray rings for Train B). Each nozzle discharges 15.2 gpm at 40 psi pressure differential across the nozzle.

All motor operated valves are powered by the 480V ES MCC's.

M.1.2 SYSTEM OPERATION

The valves in the spray lines are opened by an ESAS signal if the containment pressure rises above 4 psig. The spray pumps are started by ESAS when the containment pressure reaches 30 psig. This is assumed to occur after a large LOCA. A small LOCA may not raise the containment pressure enough to actuate the sprays. However, if the sprays are needed, they can be actuated manually.

Upon low-level alarm in the BWST, the operator must start the recirculation phase by opening the sump valves and closing the BWST outlet valves (see also Appendix K). The operator is then required to throttle the spray flow to 1200 gpm by means of valve BSV-3 (BSV-4 in Train B). This flow rate corresponds to the NPSH of 22.5 feet available from the sump (a flow rate of 1500 gpm requires a NPSH of 24.8 feet).

High and low flows are alarmed in the control room. The alarm set points are automatically transferred to the lower recirculation values when the suction is reconfigured to the sump. The spray pumps are alarmed for high motor and pump bearing temperature, and for high motor starter temperature.

The spray pumps are tested on a staggered basis once a month. Testing is governed by procedure SP-340. During the test, water from the BWST is recirculated by opening valves BSV-28 and BSV-5 or BSV-6, depending on which pump is tested. All valves in the spray flow path are stroked once a quarter. Pump testing verifies position of BSV-17 and -16 and operability of BSV-1 and -8.

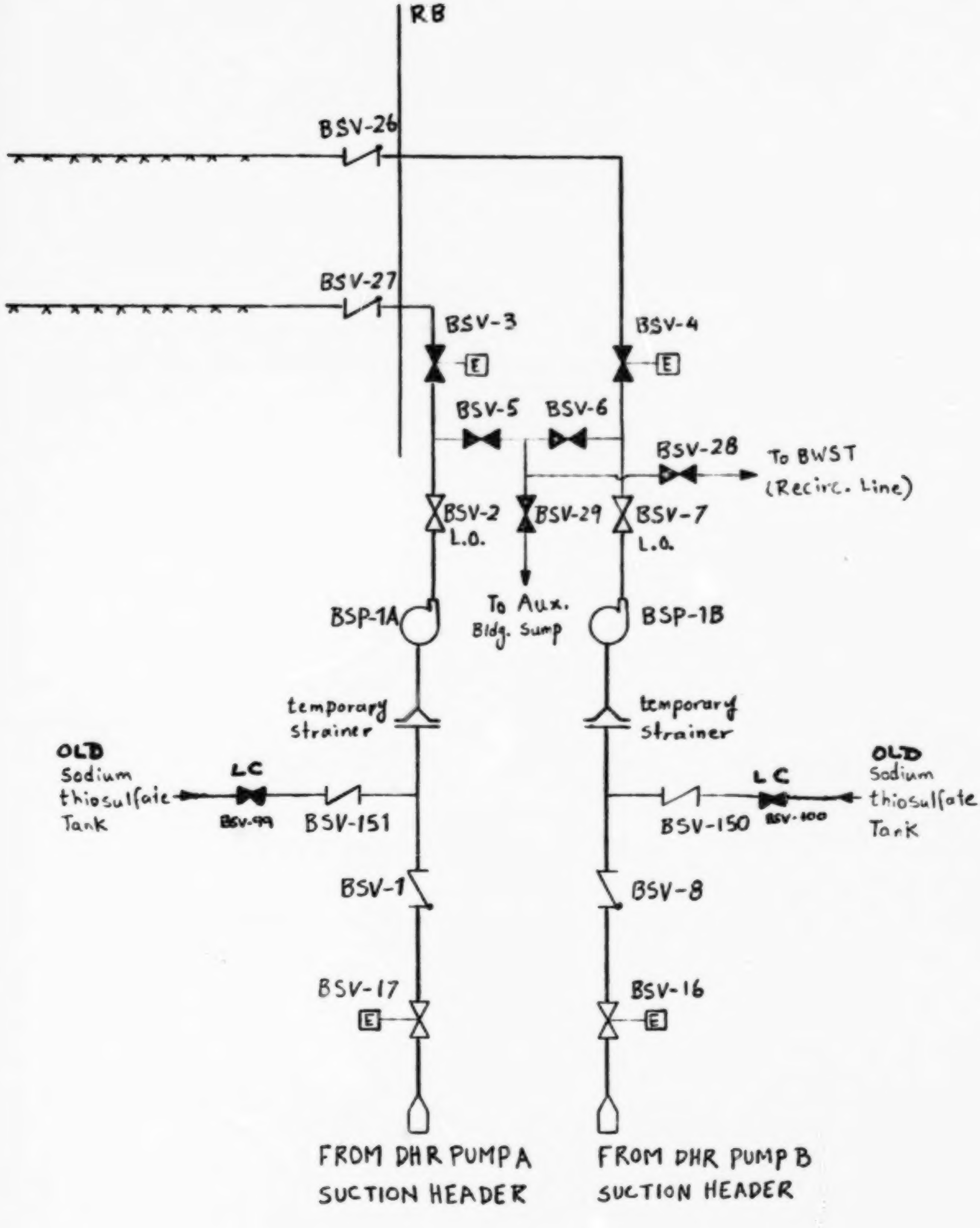

RB
BSV-26
BSV-27
BSV-3
BSV-4
E
E
BSV-5
BSV-6
BSV-28
To BWST
(Recirc. Line)
BSV-2
L.O.
BSV-29
BSV-7
L.O.
To Aux.
Bldg. Sump
BSP-1A
BSP-1B
temporary
Strainer
temporary
Strainer
OLD
Sodium
thiosulfate
Tank
LC
BSV-99
BSV-151
BSV-150
LC
BSV-100
OLD
Sodium
thiosulfate
Tank
BSV-1
BSV-8
BSV-17
E
BSV-16
E
FROM DHR PUMP A
SUCTION HEADER
FROM DHR PUMP B
SUCTION HEADER

Figure M.1 Reactor Building Spray System Schematic Diagram

M.2 SIMPLIFIED FAULT TREE

A detailed fault tree was originally drawn for failure of the Reactor Building Spray System Train A. The tree included the injection and the recirculation phase. The fault tree for Train B is identical, except for corresponding component number differences.

The detailed tree then was simplified and separated into two trees, one for the injection phase and one for the recirculation phase.

The top events are defined as:

> Failure of Both Sprays, Injection - failure of at least one spray train to deliver rated flow at the rated head to its respective spray nozzles while taking suction from the BWST, Figure M.2.
>
> Failure of Both Sprays, Recirculation - failure to successfully reconfigure at least one spray train or failure to deliver rated flow at the rated head to the train's spray nozzles for 24 hours, while taking suction from the containment sump, Figure M.3.

Failure of the sprays will also fail the function of iodine removal from the containment atmosphere.

MAJOR ASSUMPTIONS

The assumptions used to construct the detailed fault tree for the RBSS are listed below:

(1) The spray system is a normally inactive system and therefore may be unavailable on demand due to maintenance, test, or improper configuration of valves. BSV-3 and 17 are motor operated valves. BSV-2 is locked open (SP-381). The valves on the cooling lines to the pumps DCV-115, 116, 27, and 33 are locked open (SP-381). BSV-2 is a manual blocking valve, locally indicated. BSV-3 and 17 are indicated in the control room.

(2) Technical Specification 3.6.2.1 requires two spray trains to be operable. If only one is operable, the plant must be shut down in 72 hours. Plant procedure SP-347 requires valves in the flow path to be checked for position every month. Plant procedures also require the pump to be started once a month and BSV-3 and 17 stroked once a quarter. The two spray trains are tested on an alternating basis, i.e., one every two weeks. The pump is tested by opening valves BSV-28 and BSV-5 (BSV-28 and BSV-6 for BSP-1B). Flow is diverted to the BWST.

(3) It was assumed that if cooling is lost to BSP-1A, the pump will fail immediately. This is a conservative assumption. The motor and the bearing both require cooling. All faults for the cooling function can be classified as either those which prevent flow or those which prevent heat rejection from the DHCCCS. If faults occur which prevent flow to the motor or bearing, the water in the motor or bearing will quickly heat up and in very short order the motor will short or the bearing will seize. This is particularly true in the recirculation phase where the pumped water is hotter than the motor coolant. If faults occur which prevent heat rejection from the DHCCCS, but allow flow to the pump cooler, the pump may run for some time before it fails. This is particularly true for the injection phase, when there is no heat removal from DHHE-1A. The thermal inertia of the DHCCCS may be sufficient to allow continued operation of the spray pump.

(4) The spray nozzles cannot become plugged while they are inactive.

(5) The operator must reduce the system flow rate from 1500 gpm to 1200 gpm by throttling BSV-3 shortly after switchover to recirculation to prevent cavitation. The NPSH required to provide a flow rate of 1500 gpm is 24.8 feet. When operating in the recirculation mode, the NPSH available to the BS pumps is only 22.5 feet. If the operator switches to recirculation based on sump height and not BWST level, and premises the switchover on DH pump NPSH requirements, the BS pumps may cavitate even if the flow rate is reduced to 1200 gpm. Cavitation was assumed to cause pump failure. Although the sprays have two independent loops, throttling of BSV-3 and BSV-4 will be done simultaneously. They are considered to be a single operator action. "Failure to throttle the valve correctly" includes:

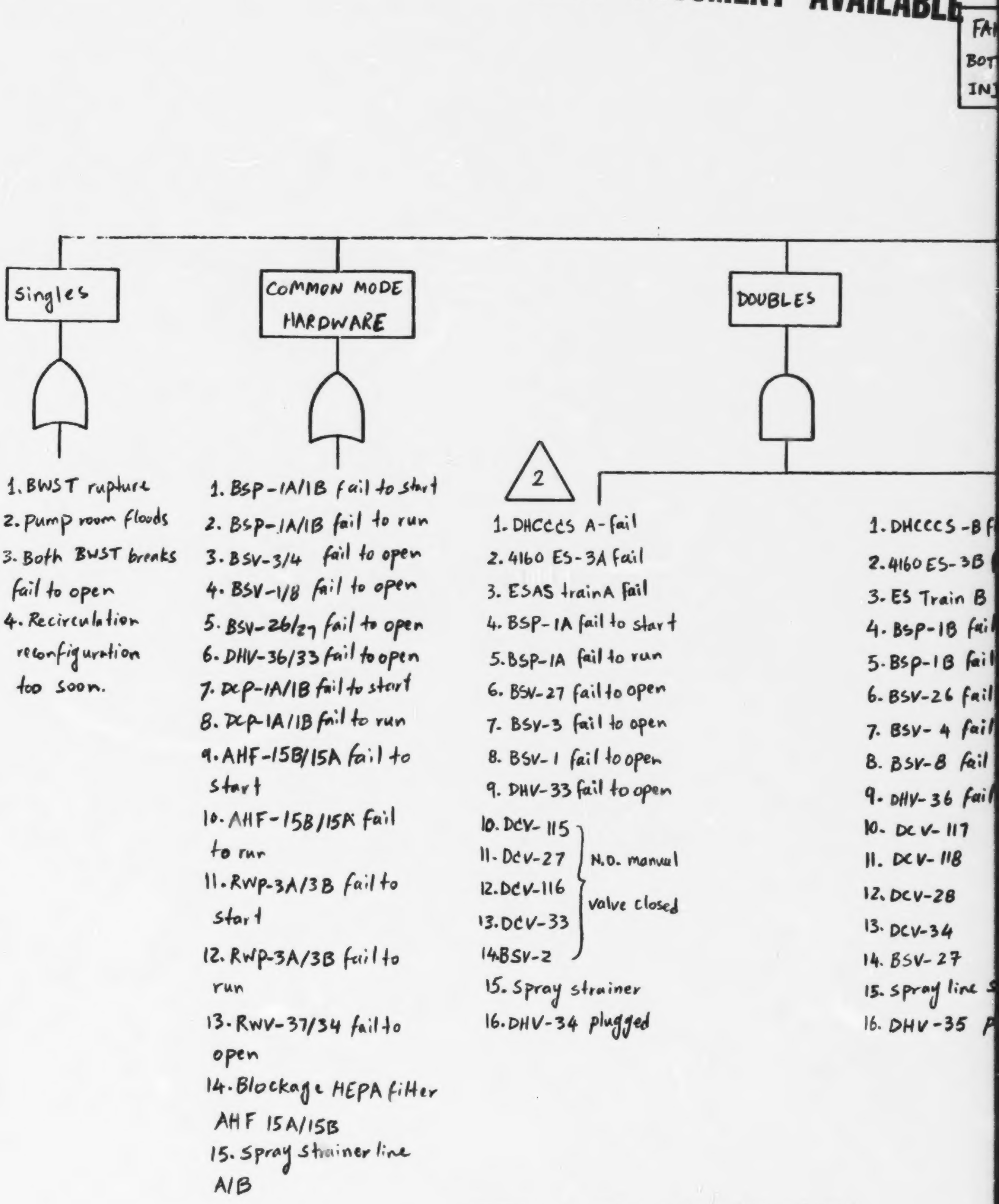
- throttling too much to starve flow,
- throttling too little to cause cavitation,
- not throttling at all.

Switching on sump level rather than on BWST level is a fault because the sump may not contain sufficient water (NPSH) to prevent pump cavitation and subsequent failure of the pumps.

(6) Upon changing from the injection phase to the recirculation phase, the entire spray system will experience a thermal shock. The BWST water is about 70°F while the reactor building sump water is about 280°F. The amount of mixing between the two streams during reconfiguration is not known. The FSAR and personnel contacts at B&W claim the spray pumps have been designed and qualified for this transient. The pump is also qualified at the higher temperature.

(7) Components, lines, and valves that were considered to be insignificant were omitted from the fault tree.

BEST DOCUMENT AVAILABLE



1. BWST rupture
2. Pump room floods
3. Both BWST breaks fail to open
4. Recirculation reconfiguration too soon.

1. BSP-1A/1B fail to start
2. BSP-1A/1B fail to run
3. BSV-3/4 fail to open
4. BSV-1/8 fail to open
5. BSV-26/27 fail to open
6. DHV-36/33 fail to open
7. DCP-1A/1B fail to start
8. DCP-1A/1B fail to run
9. AHF-15B/15A fail to start
10. AHF-15B/15A fail to run
11. RWP-3A/3B fail to start
12. RWP-3A/3B fail to run
13. RWV-37/34 fail to open
14. Blockage HEPA filter AHF 15A/15B
15. Spray strainer line A/B

1. DHCCCS A-fail
2. 4160 ES-3A fail
3. ESAS train A fail
4. BSP-1A fail to start
5. BSP-1A fail to run
6. BSV-27 fail to open
7. BSV-3 fail to open
8. BSV-1 fail to open
9. DHV-33 fail to open
10. DCV-115
11. DCV-27
12. DCV-116
13. DCV-33
14. BSV-2

} N.O. manual valve closed

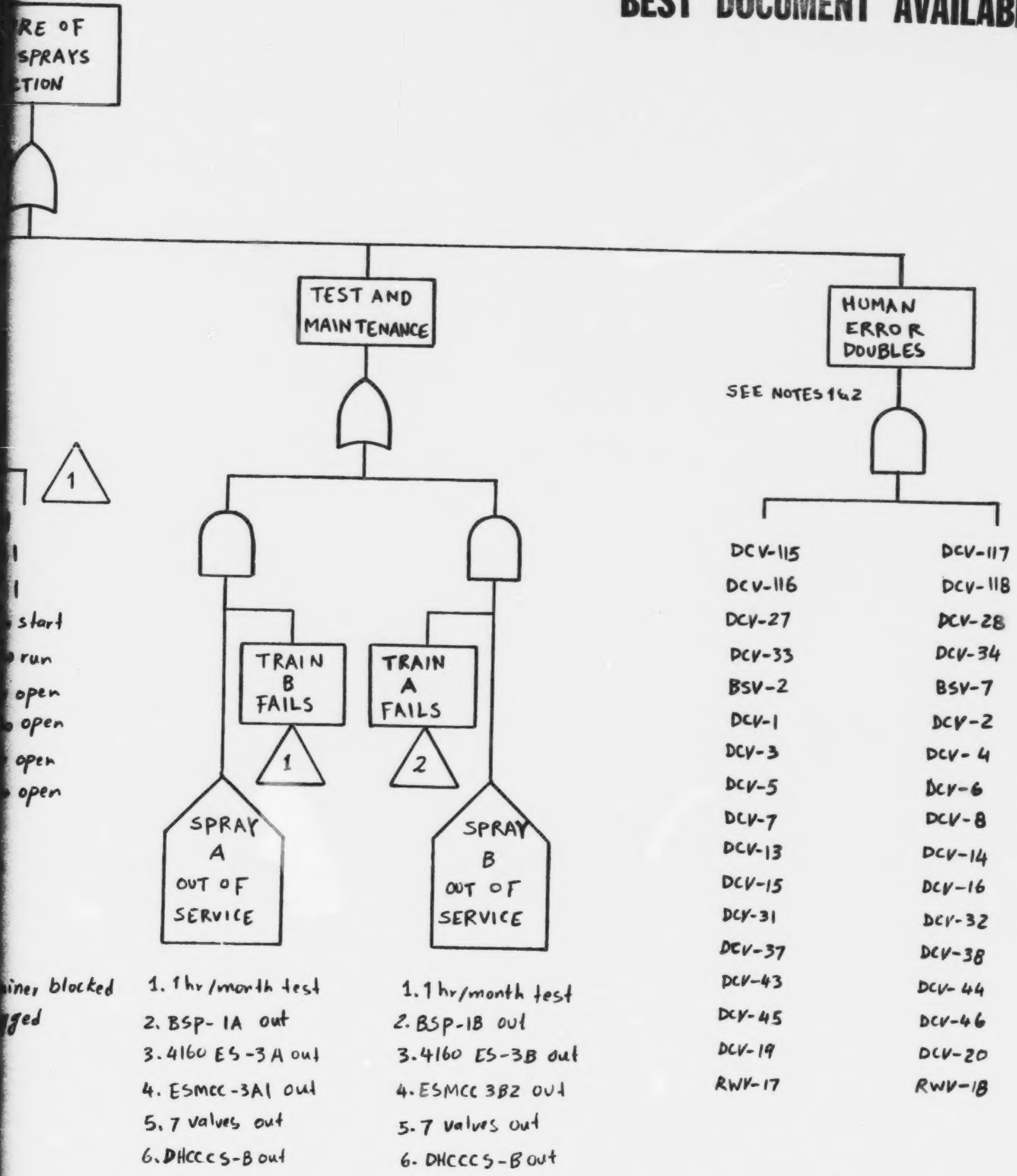
15. Spray strainer
16. DHV-34 plugged

1. DHCCCS -B f
2. 4160 ES-3B
3. ES Train B
4. BSP-1B fai
5. BSP-1B fail
6. BSV-26 fail
7. BSV- 4 fail
8. BSV-8 fail
9. DHV-36 fail
10. DCV-117
11. DCV-118
12. DCV-28
13. DCV-34
14. BSV-27
15. spray line S
16. DHV-35 P

NOTES: 1. N.O. valves left closed

2. Each event should be considered only combination with the event across f

BEST DOCUMENT AVAILABLE



RE OF
SPRAYS
TION
TEST AND MAINTENANCE
HUMAN ERROR DOUBLES
SEE NOTES 1&2
1
start
run
open
open
open
open
TRAIN B FAILS
1
TRAIN A FAILS
2
SPRAY A OUT OF SERVICE
SPRAY B OUT OF SERVICE
iner, blocked
gged
1. 1 hr/month test
2. BSP-1A out
3. 4160 ES-3A out
4. ESMCC-3A1 out
5. 7 valves out
6. DHCCCS-B out
1. 1 hr/month test
2. BSP-1B out
3. 4160 ES-3B out
4. ESMCC 3B2 out
5. 7 valves out
6. DHCCCS-B out
DCV-115
DCV-116
DCV-27
DCV-33
BSV-2
DCV-1
DCV-3
DCV-5
DCV-7
DCV-13
DCV-15
DCV-31
DCV-37
DCV-43
DCV-45
DCV-19
RWV-17
DCV-117
DCV-118
DCV-28
DCV-34
BSV-7
DCV-2
DCV-4
DCV-6
DCV-8
DCV-14
DCV-16
DCV-32
DCV-38
DCV-44
DCV-46
DCV-20
RWV-18

Figure M.2 Simplified Fault Tree - RBSS (Injection)

it.

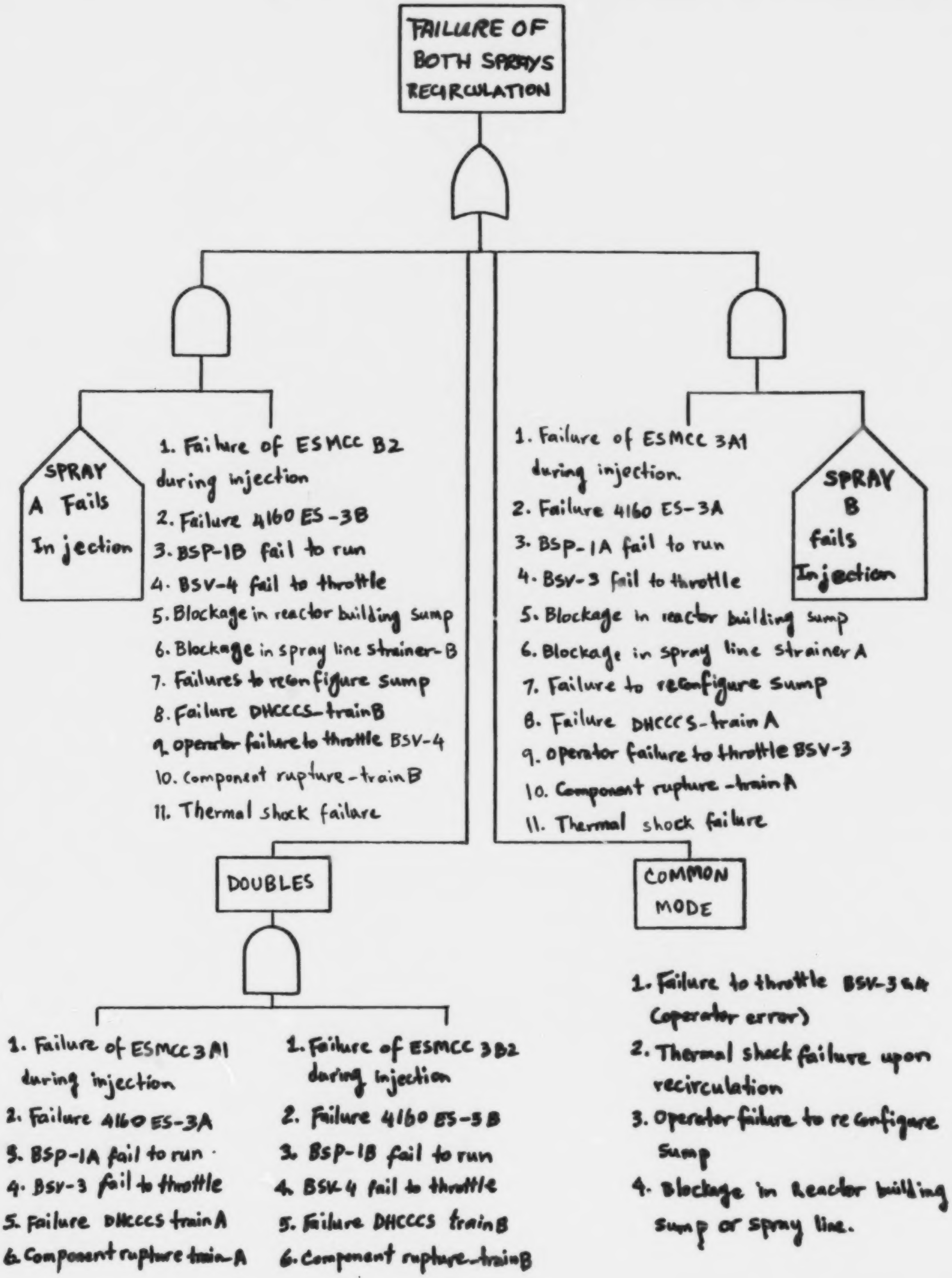

FAILURE OF BOTH SPRAYS RECIRCULATION
SPRAY A Fails Injection
1. Failure of ESMCC B2 during injection
2. Failure 4160 ES-3B
3. BSP-1B fail to run
4. BSV-4 fail to throttle
5. Blockage in reactor building sump
6. Blockage in spray line strainer-B
7. Failures to reconfigure sump
8. Failure DHCCCS-train B
9. operator failure to throttle BSV-4
10. Component rupture-train B
11. Thermal shock failure
1. Failure of ESMCC 3A1 during injection.
2. Failure 4160 ES-3A
3. BSP-1A fail to run
4. BSV-3 fail to throttle
5. Blockage in reactor building sump
6. Blockage in spray line strainer A
7. Failure to reconfigure sump
8. Failure DHCCCS-train A
9. operator failure to throttle BSV-3
10. Component rupture-train A
11. Thermal shock failure
SPRAY B fails Injection
DOUBLES
COMMON MODE
1. Failure of ESMCC 3A1 during injection
2. Failure 4160 ES-3A
3. BSP-1A fail to run
4. BSV-3 fail to throttle
5. Failure DHCCCS train A
6. Component rupture train-A
1. Failure of ESMCC 3B2 during injection
2. Failure 4160 ES-3B
3. BSP-1B fail to run
4. BSV-4 fail to throttle
5. Failure DHCCCS train B
6. Component rupture-train B
1. Failure to throttle BSV-3 & 4 (operator error)
2. Thermal shock failure upon recirculation
3. Operator failure to reconfigure Sump
4. Blockage in Reactor building sump or spray line.

Figure M.3 Simplified Fault Tree - RBSS (Recirculation)

[redacted]

M.3 SYSTEM QUANTIFICATION

M.3.1 SYSTEM RELIABILITY CHARACTERISTICS

For cases where offsite power is available the major contributors to the unavailability of the RBSS during the injection phase are operator errors. For large LOCAs (B1, B2) the dominant contributor is that the operator reconfigures for recirculation too soon. For small LOCAs (B3, B4) an additional operator error of the same order of magnitude can occur: failure to manually initiate the sprays when required.

In the case that offsite power is not available, the failure of both diesels to start and unavailability of power from fossil units CR-1 and -2 (the unavailability of both fossil units was assessed as 0.36) is about an order of magnitude smaller than the probability of the first two operator errors described.

The unavailability of the RBSS during the recirculation phase is dominated by two operator errors. The first is that the operator fails to reconfigure the suction to the reactor building sump for recirculation. The second dominant contribution is that the operator fails to throttle the spray valves to prevent pump cavitation. About two orders of magnitude smaller are the contributions of nonrecoverable hardware faults during the injection phase (or a maintenance outage) in one train combined with hardware faults that occur during the recirculation phase in the other train. These failures include the DHCCCS that supplies pump cooling.

M.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

This section presents the quantification of the RBSI* unavailability for required emergency operation of the RBSS during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree was transformed into a modularized fault tree.

Table M.1 shows the RBSS success requirements, Table M.2 contains the top event definition for the modularized fault tree, and Figures M.4 through M.7 show the modularized fault trees for the RBSI. The unavailability of each gate is shown on the tree. Table M.3 shows the Boolean equations that represent the fault trees. Table M.4 shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table M.5 presents a summary of the point estimates for each gate.

---

*RBSI; Reactor Building Spray System - Injection Phase.

Table M.1 Containment Spray Injection

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4	1/2 Trains	1,2,3

NOTES: 1 Success definition is the same for all LOCA sizes.

2 The time into the accident sequence when containment spray (CS) will be required is dependent on the size of the LOCA. However, it was assumed that CS would be required during the injection phase for all LOCA sizes

3 The containment spray system is used both for containment atmosphere heat removal and post accident radioactivity removal.

Table M.2 Containment Spray Injection - Top Events

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
CSA	Failure of containment spray Train A to provide containment atmosphere cooling.	
CSB	Failure of containment spray Train B to provide containment atmosphere cooling.	
CSI	Failure of both containment spray trains to provide containment atmosphere cooling.	

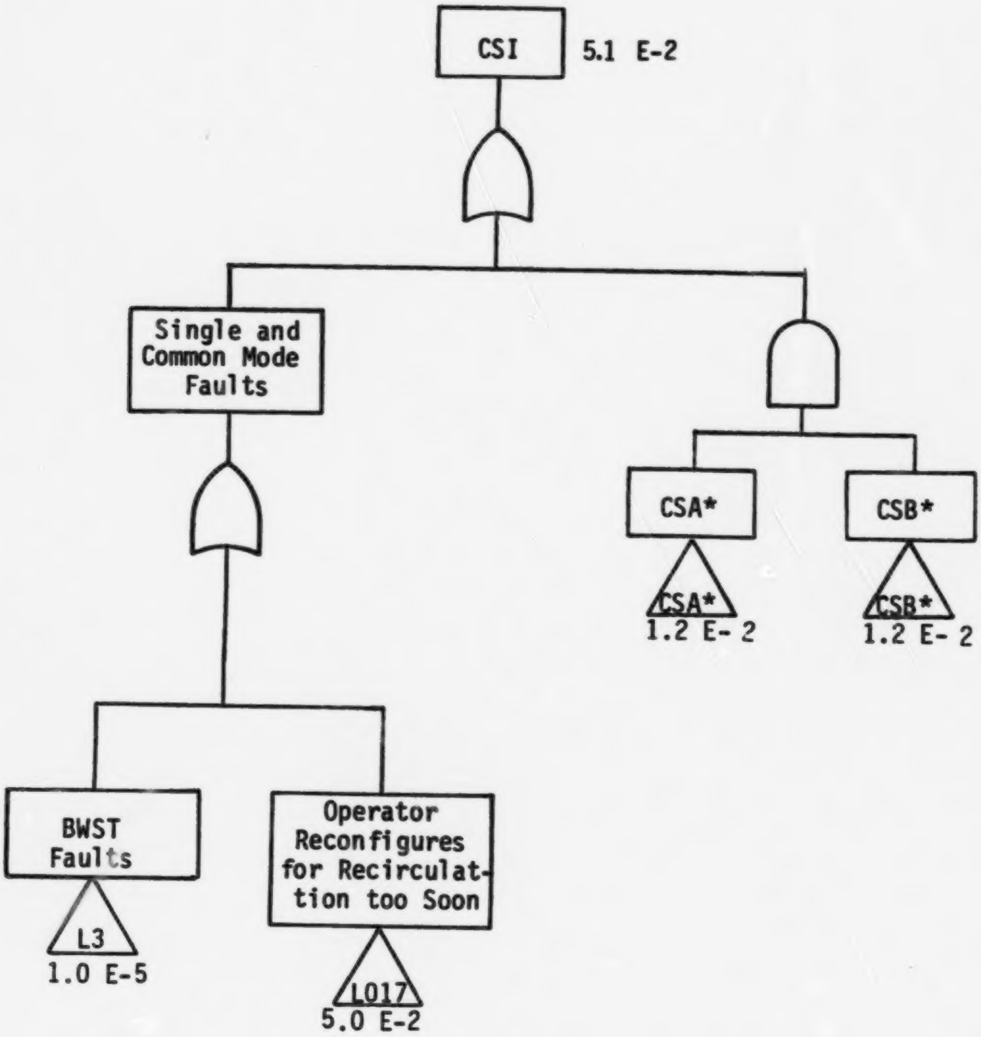

CSI
5.1 E-2
Single and Common Mode Faults
CSA*
CSB*
CSA*
1.2 E- 2
CSB*
1.2 E- 2
BWST Faults
Operator Reconfigures for Recirculation too Soon
L3
1.0 E-5
LO17
5.0 E-2

Figure M.4 Modularized Fault Tree for Event "CSI"; B_1 and B_2-LOCA

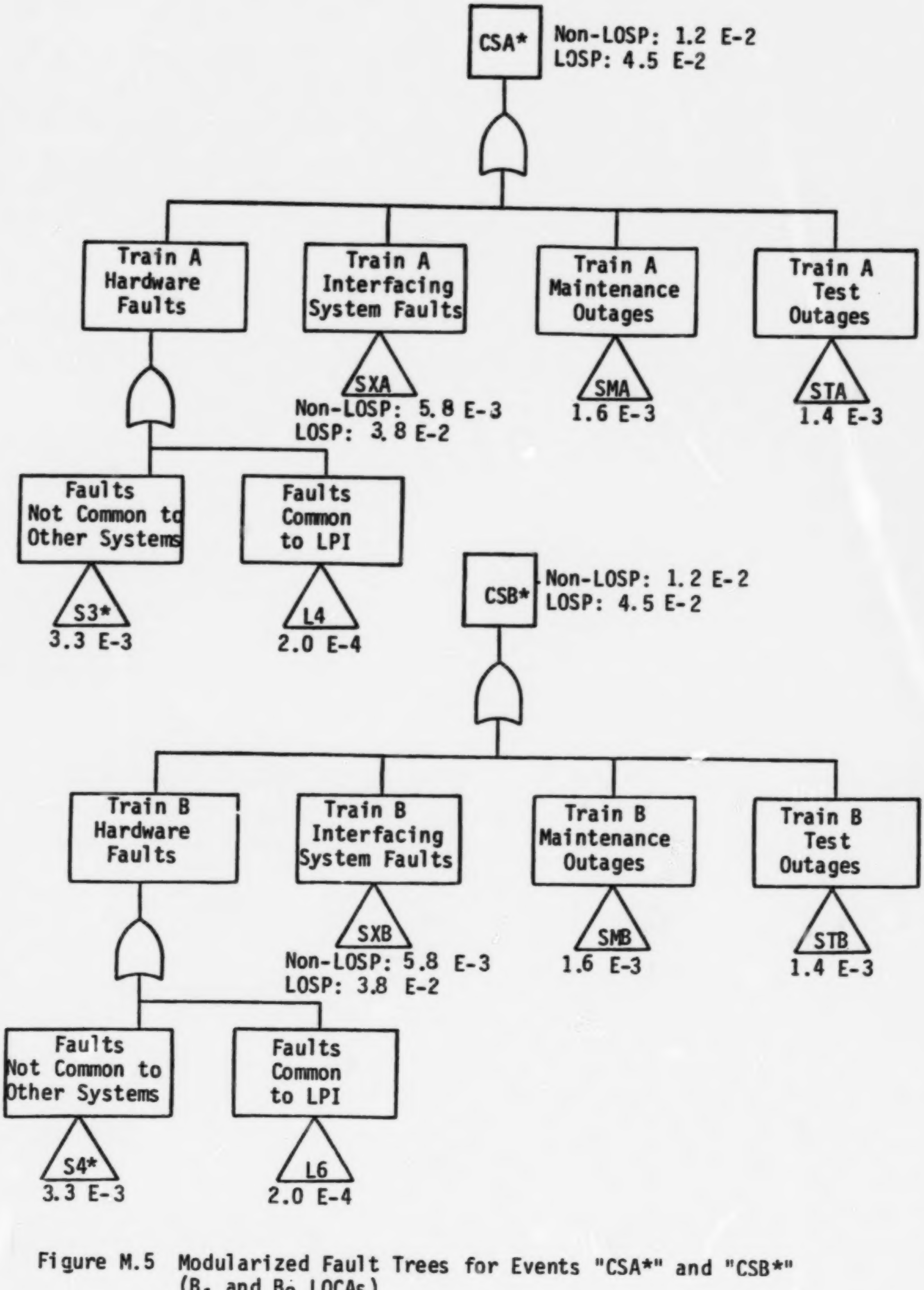
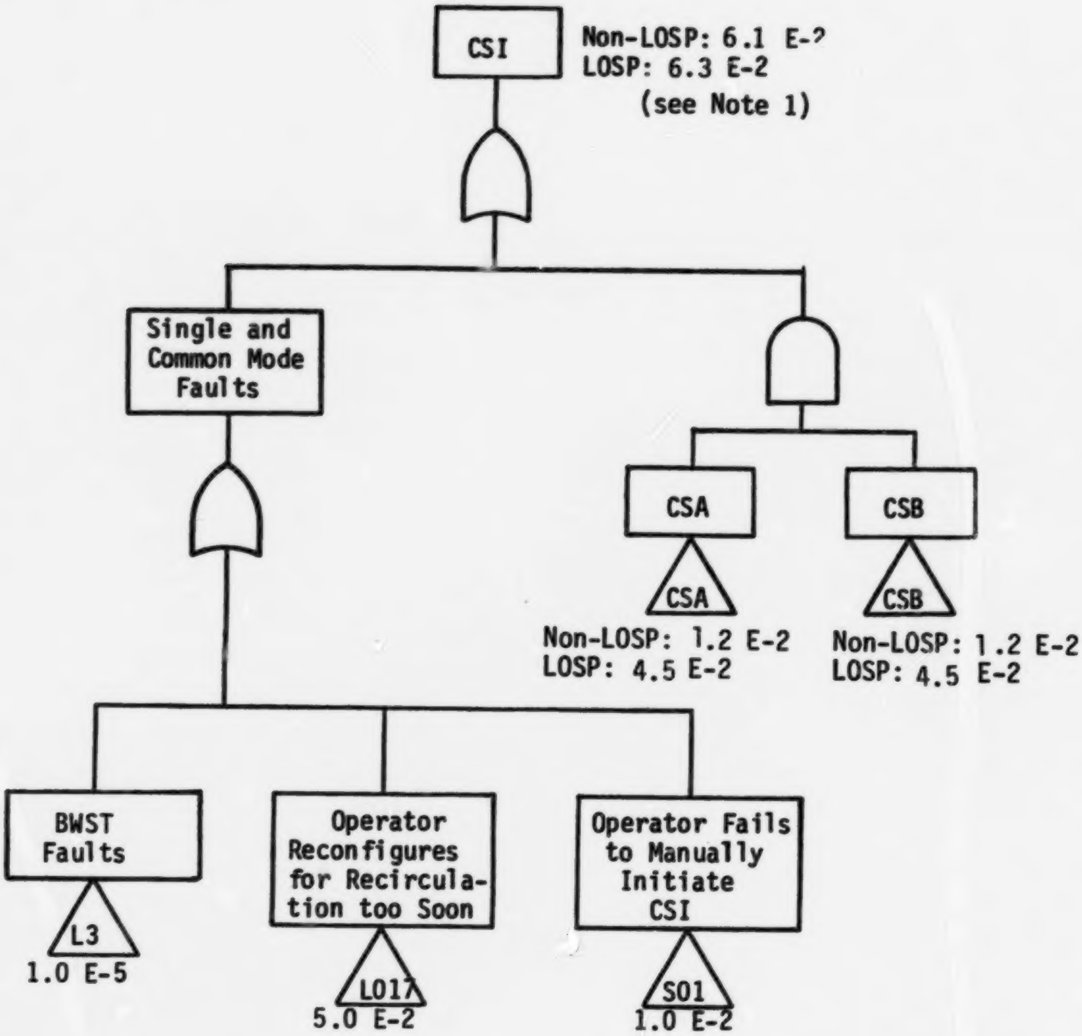

CSA*
Non-LOSP: 1.2 E-2
LOSP: 4.5 E-2
Train A Hardware Faults
Train A Interfacing System Faults
Train A Maintenance Outages
Train A Test Outages
SXA
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
SMA
1.6 E-3
STA
1.4 E-3
Faults Not Common to Other Systems
Faults Common to LPI
S3*
3.3 E-3
L4
2.0 E-4
CSB*
Non-LOSP: 1.2 E-2
LOSP: 4.5 E-2
Train B Hardware Faults
Train B Interfacing System Faults
Train B Maintenance Outages
Train B Test Outages
SXB
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
SMB
1.6 E-3
STB
1.4 E-3
Faults Not Common to Other Systems
Faults Common to LPI
S4*
3.3 E-3
L6
2.0 E-4

Figure M.5 Modularized Fault Trees for Events "CSA*" and "CSB*" (B_1 and B_2 LOCAs)


CSI
Non-LOSP: 6.1 E-2
LOSP: 6.3 E-2
(see Note 1)
Single and Common Mode Faults
CSA
CSB
CSA
CSB
Non-LOSP: 1.2 E-2
LOSP: 4.5 E-2
Non-LOSP: 1.2 E-2
LOSP: 4.5 E-2
BWST Faults
Operator Reconfigures for Recirculation too Soon
Operator Fails to Manually Initiate CSI
L3
1.0 E-5
L017
5.0 E-2
S01
1.0 E-2

NOTE 1. The Non-LOSP probability applies to both the B_3 and B_4 LOCA cases. The LOSP probability applies only to the transient-induced B_4 LOCA.

Figure M.6 Modularized Fault Tree for Event "CSI"; B_3 and B_4-LOCA

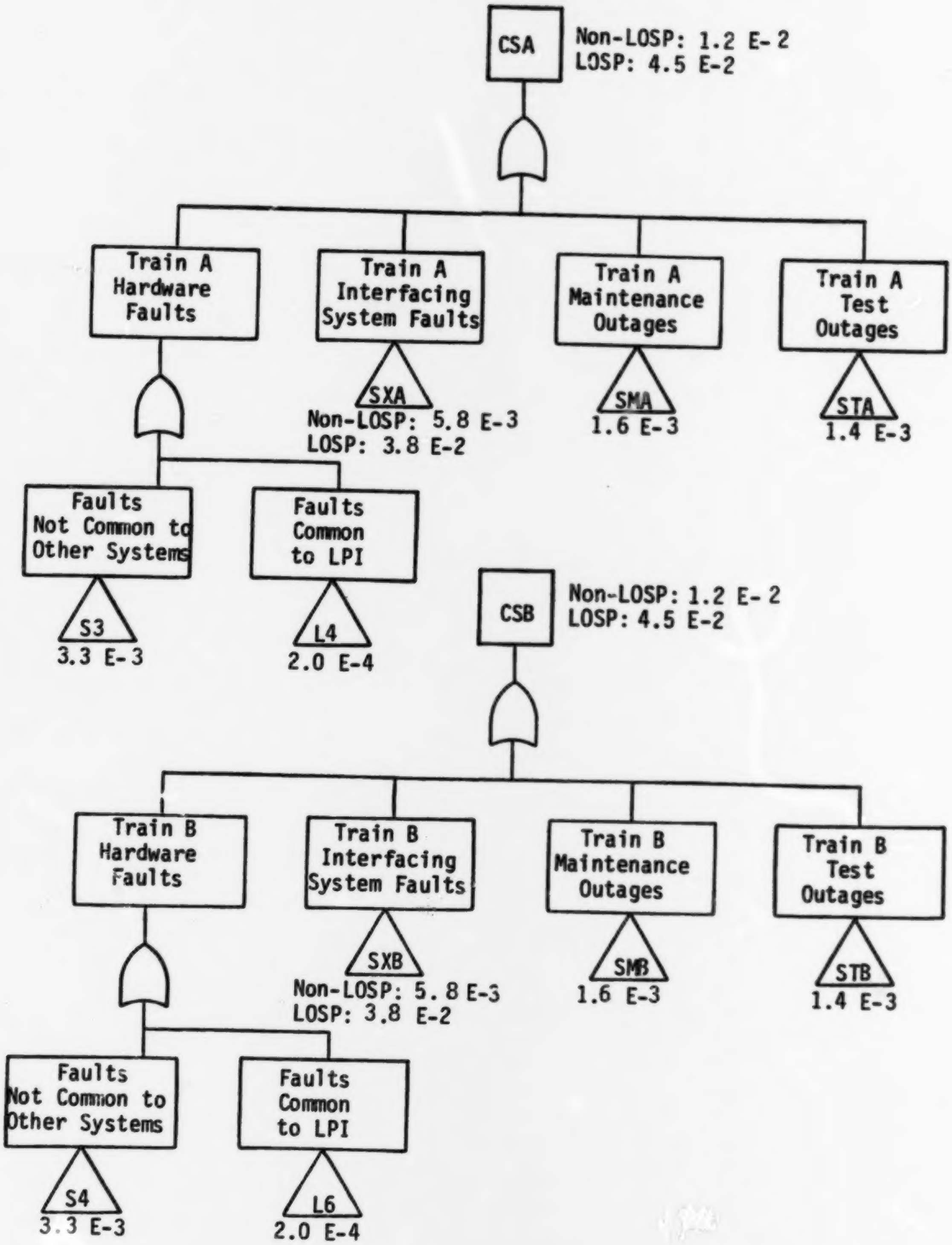

CSA
Non-LOSP: 1.2 E- 2
LOSP: 4.5 E-2
Train A Hardware Faults
Train A Interfacing System Faults
Train A Maintenance Outages
Train A Test Outages
SXA
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
SMA
1.6 E-3
STA
1.4 E-3
Faults Not Common to Other Systems
Faults Common to LPI
S3
3.3 E-3
L4
2.0 E-4
CSB
Non-LOSP: 1.2 E- 2
LOSP: 4.5 E-2
Train B Hardware Faults
Train B Interfacing System Faults
Train B Maintenance Outages
Train B Test Outages
SXB
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
SMB
1.6 E-3
STB
1.4 E-3
Faults Not Common to Other Systems
Faults Common to LPI
S4
3.3 E-3
L6
2.0 E-4

Figure M.7 Modularized Fault Trees for Events "CSA" and "CSB"; (B_3 and B_4 LOCAs)

Table M.3 (1/2) Containment Spray Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS — NOTES

B3, B4 - LOCAs

CSI3 = CSI4 = SO1 + LO17 + L3 + CSA·CSB — 1

B1, B2 - LOCAs

CSI1 = CSI2 = LO17 + L3 + CSA*·CSB* — 1

INTERMEDIATE EVENTS

CSA = L4 + S3 + SXA + SMA + STA
CSB = L6 + S4 + SXB + SMB + STB

SXA = DA + ACA — 2
SXB = DB + ACB — 2

CSA* = L4 + S3* + SXA + SMA + STA
CSB* = L6 + S4* + SXB + SMB + STB

NOTES: 1. Terms representing simultaneous outages in both legs are to be omitted since they are prohibited by Technical Specifications.

2. For offsite power available only DA and DB, respectively, contribute quantitatively. For loss of offsite power initiator ACA and ACB will be contained in DA and DB, respectively, and require a further Boolean reduction; see fault tree analysis of the DHCCCS. DC-contribution contained in ACA and ACB.

Table M.3 (2/2) Containment Spray Injection (Cont.)

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

B3, B4 - LOCAs

$$
\begin{aligned}
\mathrm{CSI3} = \mathrm{CSI4} = {} & \mathrm{S01} + \mathrm{L017} + \mathrm{L3} + (\mathrm{S3}\cdot\mathrm{S4}) + (\mathrm{L4}\cdot\mathrm{L6}) + (\mathrm{ACA}\cdot\mathrm{ACB}) + \\
& + \mathrm{ACA}\cdot(\mathrm{DB} + \mathrm{S4} + \mathrm{L6} + \mathrm{SMB} + \mathrm{STB}) + \mathrm{ACB}\cdot(\mathrm{DA} + \mathrm{S3} + \mathrm{L4} + \mathrm{SMA} + \mathrm{STA}) + \\
& + (\mathrm{DA}\cdot\mathrm{DB}) + \mathrm{DA}\cdot(\mathrm{S4} + \mathrm{L6} + \mathrm{SMB} + \mathrm{STB}) + \mathrm{DB}\cdot(\mathrm{S3} + \mathrm{L4} + \mathrm{SMA} + \mathrm{STA}) + \\
& + \mathrm{S3}\cdot(\mathrm{L6} + \mathrm{SMB} + \mathrm{STB}) + \mathrm{S4}\cdot(\mathrm{L4} + \mathrm{SMA} + \mathrm{STA}) + \mathrm{L4}\cdot(\mathrm{SMB} + \mathrm{STB}) + \\
& + \mathrm{L6}\cdot(\mathrm{SMA} + \mathrm{STA})
\end{aligned}
$$

B1, B2 - LOCAs

$$
\begin{aligned}
\mathrm{CSI1} = \mathrm{CSI2} = {} & \mathrm{L017} + \mathrm{L3} + (\mathrm{S3}^{*}\cdot\mathrm{S4}^{*}) + (\mathrm{L4}\cdot\mathrm{L6}) + (\mathrm{ACA}\cdot\mathrm{ACB}) + \mathrm{ACA}\cdot \\
& \cdot(\mathrm{DB} + \mathrm{S4}^{*} + \mathrm{L6} + \mathrm{SMB} + \mathrm{STB}) + \mathrm{ACB}\cdot(\mathrm{DA} + \mathrm{S3}^{*} + \mathrm{L4} + \mathrm{SMA} + \mathrm{STA}) + \\
& + (\mathrm{DA}\cdot\mathrm{DB}) + \mathrm{DA}\cdot(\mathrm{S4}^{*} + \mathrm{L6} + \mathrm{SMB} + \mathrm{STB}) + \mathrm{DB}\cdot(\mathrm{S3}^{*} + \mathrm{L4} + \mathrm{SMA} + \mathrm{STA}) + \\
& + \mathrm{S3}^{*}\cdot(\mathrm{L6} + \mathrm{SMB} + \mathrm{STB}) + \mathrm{S4}^{*}\cdot(\mathrm{L4} + \mathrm{SMA} + \mathrm{STA}) + \mathrm{L4}\cdot(\mathrm{SMB} + \mathrm{STB}) + \\
& + \mathrm{L6}\cdot(\mathrm{SMA} + \mathrm{STA})
\end{aligned}
$$

Table M.4 (1/10) Event "CSI" Quantification; B_1 and B_2 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L3		BWST FAULTS			1.0 E-5			6, 7
L017	OPERATOR	SWITCHES TO RECIRCULATION TOO SOON			5.0 E-2	3^+, 10^-	0	6, 7
$S3^{*} \cdot S4^{*}$		PRODUCT INCLUDING COUPLED PUMP AND CHECK VALVE FAILURE			2.6 E-4	2^+, 2^-	B	9

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.4 (2/10) Event "CSA*" Quantification; B_1 and B_2 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S3*		TRAIN A HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			10
	PUMP BSP-1A	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	PUMP BSP-1A	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	$10^+, 10^-$		
	CHECK VALVE BSV-27	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		
	MOV BSV-3	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CHECK VALVE BSV-1	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		
	MOV BSV-17	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4	$3^+, 3^-$		
	SPRAY STRAINER	NOT REMOVED			ε			
	VALVE DCV-115	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-27	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-116	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-33	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE BSV-2	LEFT CJOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
					Σ=3.3 E-3			
	ILS·S02	ESAS TRAIN A FAILS AND OPERATOR FAILS TO RECOVER						
	ILS	ESAS TRAIN A FAILS	D		1.1 E-4			
	S02	OPERATOR FAILS TO RECOVER	D		1.0 E-2			
					π=1.1 E-6			
					Σ=3.3 E-3			
L4		TRAIN A HARDWARE FAULTS COMMON TO LPI			2.0 E-4			2
SXA		TRAIN A INTERFACING SYSTEM FAULTS						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
DA		DHCCCS TRAIN A FAULTS (INSUFFICIENT COOLING)						
		NON LOSP			5.8 E-3			3
		LOSP			3.8 E-2			

Table M.4 (3/10) Event "CSA*" Quantification; B_1 and B_2 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ACA		AC TRAIN A (INSUFFICIENT POWER)						
		NON LOSP			ϵ			
		LOSP			3.2 E-2			4
DCA		DC TRAIN A (INSUFFICIENT POWER)						
		NON LOSP			ϵ			
		LOSP			3.2 E-3			5
SMA		TRAIN A MAINTENANCE OUTAGES			1.6 E-3	3^+, 3^-	M	
	PUMP BSP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
	MOV BSV-3	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
	MOV BSV-17	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
					Σ=1.6 E-3			
STA		TRAIN A TEST OUTAGE	1/720	1	1.4 E-3		T	

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.4 (4/10) Event "CSB*" Quantification; B_1 and B_2 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S4*		TRAIN B HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			10
	PUMP BSP-1B	FAILS TO START	D		1.0 E-3	3^+, 3^-		
	PUMP BSP-1B	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	10^+, 10^-		
	CHECK VALVE BSV-26	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	MOV BSV-4	FAILS TO OPEN	D		1.0 E-3	3^+, 3^-		
	CHECK VALVE BSV-8	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	MOV BSV-16	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4	3^+, 3^-		
	SPRAY STRAINER	BLOCKED OR PLUGGED			ε			
	VALVE DCV-117	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10^+, 10^-	H	1
	VALVE DCV-119	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10^+, 10^-	H	1
	VALVE DCV-28	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10^+, 10^-	H	1
	VALVE DCV-34	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10^+, 10^-	H	1
	VALVE BSV-7	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10^+, 10^-	H	1
					Σ=3.3 E-3			
ILS S02		ESFAS TRAIN B FAILS AND OPERATOR FAILS TO RECOVER						
	ILS	ESFAS TRAIN B FAILS	D		1.1 E-4			
	S02	OPERATOR FAILS TO RECOVER	D		1.0 E-2			
					Σ=1.1 E-6			
					Σ=3.3 E-3			
L6		TRAIN B HARDWARE FAULTS COMMON TO LPI			2.0 E-4			
SXB		TRAIN B INTERFACING SYSTEM FAULTS						2
		NON LOSP			5.8 E-3			
		LOSP			3.8 F-7			
DB		DHCCCS-B (INSUFFICIENT COOLING)						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
ACB		AC TRAIN B (INSUFFICIENT POWER)						
		NON LOSP			ε			
		LOSP			3.2 E-2			4

Table M.4 (5/10) Event "CSB*" Quantification; B_1 and B_2 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
DCB		DC TRAIN B (INSUFFICIENT POWER)						
		NON LOSP			ε			
		LOSP			3.2 E-3			5
SMB		TRAIN B MAINTENANCE OUTAGES			1.6 E-3	$3^+, 3^-$	M	
	PUMP BSP-1B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	MOV BSV-4	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	MOV BSV-16	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
					Σ=1.6 E-3			
STB		TRAIN B TEST OUTAGE	1/720	1	1.4 E-3		T	

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.4 (6/10) Event "CSI" Quantification; B_3 and B_4 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L3		BWST FAULTS			1.0 E-5			6, 7
L017	OPERATOR	SWITCHES TO RECIRCULATION TOO SOON			5.0 E-2	3^+, 10^-	0	6, 7
S01	OPERATOR	FAILS TO MANUALLY INITIATE CSI			1.0 E-2	3^+, 10^-	0	8
S3·S4		PRODUCT INCLUDING COUPLED PUMP AND CHECK VALVE FAILURE			2.6 E-4	2^+, 2^-	B	9

Table M.4 (7/10) Event "CSA" Quantification; B_3 and B_4 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S3		TRAIN A HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			11
	PUMP BSP-1A	FAILS TO START			1.0 E-3	$3^+, 3^-$		
	PUMP BSP-1A	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	$10^+, 10^-$		
	CHECK VALVE BSV-27	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		
	MOV BSV-3	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CHECK VALVE BSV-1	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		
	MOV BSV-17	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4	$3^+, 3^-$		
	SPRAY STRAINER	BLOCKED OR PLUGGED			ε			
	VALVE DCV-115	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-27	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-116	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-33	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE BSV-2	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
					Σ=3.3 E-3			
L4		TRAIN A HARDWARE FAULTS COMMON TO LPI			2.0 E-4			2
SXA		TRAIN A INTERFACING SYSTEM FAULTS						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
DA		DHCCCS TRAIN A FAULTS (INSUFFICIENT COOLING						3
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
ACA		AC TRAIN A (INSUFFICIENT POWER)						4
		NON LOSP			ε			
		LOSP			3.2 E-2			
DCA		DC TRAIN A (INSUFFICIENT POWER)						5
		NON LOSP			ε			
		LOSP			3.2 E-3			

414

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.4 (8/10) Event "CSA" Quantification; B3 and B4 LOCAS

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
SMA		TRAIN A MAINTENANCE OUTAGES			1.6 E-3	3$^+$, 3$^-$	M	
	PUMP BSP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3$^+$, 3$^-$	M	
	MOV BSV-3	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3$^+$, 3$^-$	M	
	MOV BSV-17	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3$^+$, 3$^-$	M	
					Σ=1.6 E-3			
STA		TRAIN A TEST OUTAGE	1/720	1	1.4 E-3		T	

Table M.4 (9/10) Event "CSB" Quantification; B3 and B4 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S4		TRAIN B HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			11
	PUMP BSP-1B	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	PUMP BSP-1B	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	$10^+, 10^-$		
	CHECK VALVE BSV-26	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		
	MOV BSV-4	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CHECK VALVE BSV-8	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		
	MOV BSV-16	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4	$3^+, 3^-$		
	SPRAY	BLOCKED OR PLUGGED						
	VALVE DCV-117	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-118	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-28	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE DCV-34	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
	VALVE BSV-7	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	$10^+, 10^-$	H	1
					Σ=3.3 E-3			
L6		TRAIN B HARDWARE FAULTS COMMON TO LPI			2.0 E-4			2
SXB		TRAIN B INTERFACING SYSTEM FAULTS						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
DB		DHCCCS-B -INSUFFICIENT COOLING						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			3
ACB		AC TRAIN B - INSUFFICIENT POWER						
		NON LOSP			ϵ			
		LOSP			3.2 E-2			4
DCB		DC TRAIN B - INSUFFICIENT POWER						
		NON LOSP			ϵ			
		LOSP			3.2 E-3			5

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.4 (10/10) Event "CSB" Quantification; B_3 and B_4 LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
SMB		TRAIN B MAINTENANCE OUTAGES			1.6 E-3	3^+, 3^-	M	
	PUMP BSP-1B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
	MOV BSV-4	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
	MOV BSV-1C	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
					Σ=1.6 E-3			
STB		TRAIN B TEST OUTAGE	1/720	1	1.4 E-3		T	

Table M.4 Containment Spray Injection

QUANTIFICATION TABLES

NOTES

1 This valve is closed in order to perform maintenance. Failure to reopen after maintenance would fail the train. The failure probability was assessed as (0.02) maintenance acts/month times a human error rate of (1.0 E-2). Recovery would occur on monthly CSI tests.

2 For assessment of these faults see LPI fault tree analysis, gate L4 (L6).

3 See DHCCCS fault tree analysis. For loss of offsite power case AC train A(B) is included as a fault in DA(DB).

4 See AC-power fault tree analysis.

5 See DC-power fault tree analysis

6 See low pressure injection fault tree.

7 This fault common to low pressure injection system.

8 For this size LOCA, procedures require balancing HPI flow which in turn requires defeating the ESFAS-signal. Therefore, spray initiation is manual if the system is required.

9 Check valve failures BSV-26 and BSV-27 and pumps BSP-1A and BSP-1B were assumed coupled with a β-factor of 0.1.

10 This event applies to B_1-and B_2-LOCAs only.

11 This event applies to B_3-and B_4-LOCAs only.

Table M.5 RBSI - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
S3	3.3 E-3
L4	2.0 E-4
DA	5.8 E-3* 3.8 E-2**
SMA	1.6 E-3
STA	1.4 E-3
S4	3.3 E-3
L6	2.0 E-4
DB	5.8 E-3* 3.8 E-2**
SMB	1.6 E-3
STB	1.4 E-3
S3·S4	2.6 E-4
L3	1.0 E-5
L017	5.0 E-2
S01	1.0 E-2
S3*	3.3 E-3
S4*	3.3 E-3
S3*·S4*	2.6 E-4
ACA	ε* 3.2 E-2**
ACB	ε* 3.2 E-2**
DCA	ε* 3.2 E-3**
DCB	ε* 3.2 E-3**

*Offsite power available
**Offsite power not available

M.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the RBSR* unavailability for required emergency operation of the RBSS during the recirculation phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree was transformed into a modularized fault tree.

Table M.6 shows the RBSS success requirements. Table M.7 contains the top event definition for the modularized fault tree, and Figures M.8 through M.12 show the modularized fault trees for the RBSR. The unavailability of each gate is shown on the tree. Table M.8 shows the Boolean equations that represent the fault trees. Table M.9 shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table M.10 presents a summary of the point estimates for each gate.

---

*RBSR: Reactor Building Spray System - Recirculation Phase

Table M.6 Containment Spray Recirculation

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4	1/2 trains	1,2,3

NOTES: 1. Success definition is the same for all LOCA sizes.

2. The time into the accident sequence when containment spray (CS) will be required is dependent on the size of the LOCA. However, it was assumed that CS would be required during the recirculation phase for all LOCA sizes.

3. The containment spray system is used both for containment atmosphere heat removal and post accident radioactivity removal.

Table M.7 Containment Spray Recirculation

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
CSR	Failure of both containment spray trains to provide containment atmosphere cooling during recirculation.	
CSA**	Failure of containment spray Train A to provide containment atmosphere cooling during injection.	
CSB**	Failure of containment spray Train B to provide containment atmosphere cooling during injection.	
CRA	Failure of containment spray Train A to provide containment atmosphere cooling during recirculation.	
CRB	Failure of containment spray Train B to provide containment atmosphere cooling during recirculation.	

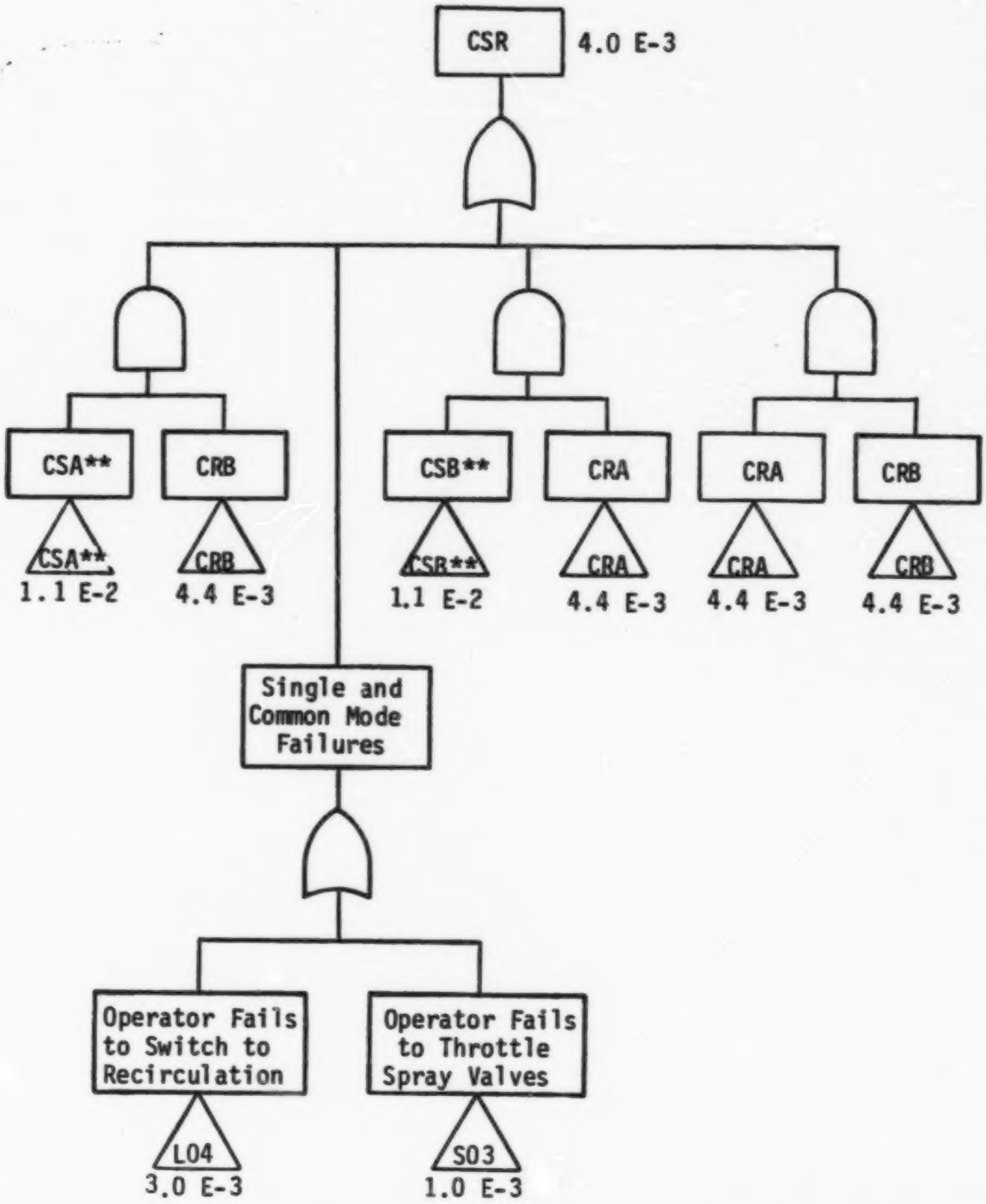

CSR
4.0 E-3
CSA**
CRB
CSB**
CRA
CRA
CRB
CSA**
1.1 E-2
CRB
4.4 E-3
CSB**
1.1 E-2
CRA
4.4 E-3
CRA
4.4 E-3
CRB
4.4 E-3
Single and Common Mode Failures
Operator Fails to Switch to Recirculation
Operator Fails to Throttle Spray Valves
L04
3.0 E-3
S03
1.0 E-3

Figure M.8 Modularized Fault Tree for Event "CSR"

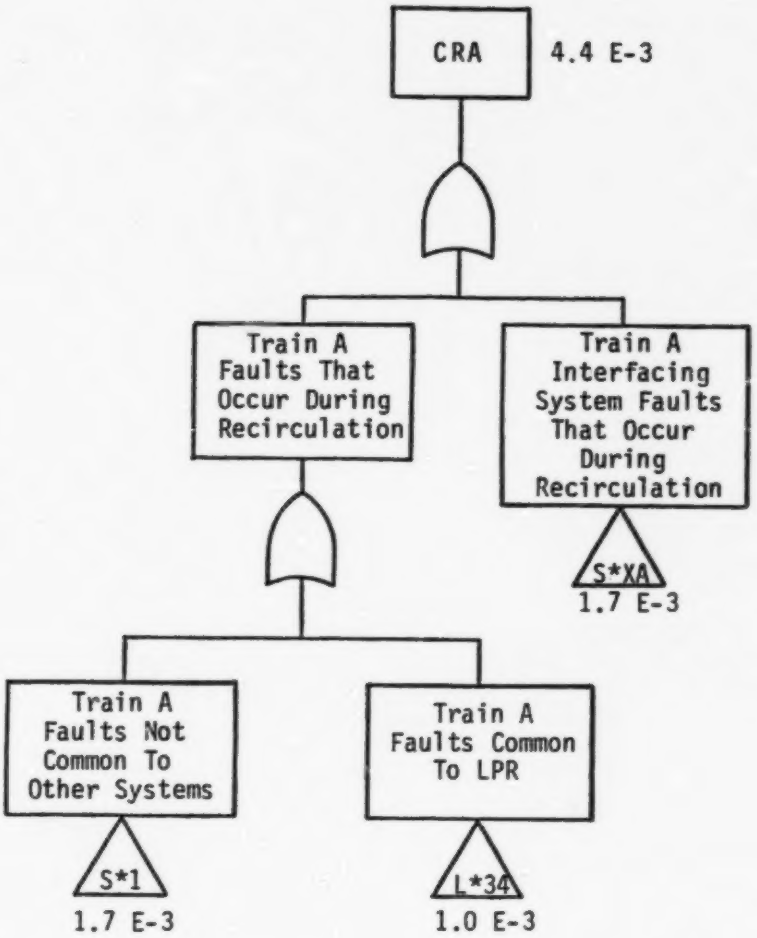

CRA
4.4 E-3
Train A Faults That Occur During Recirculation
Train A Interfacing System Faults That Occur During Recirculation
S*XA
1.7 E-3
Train A Faults Not Common To Other Systems
Train A Faults Common To LPR
S*1
1.7 E-3
L*34
1.0 E-3

Figure M.9 Modularized Fault Tree for Event "CRA"

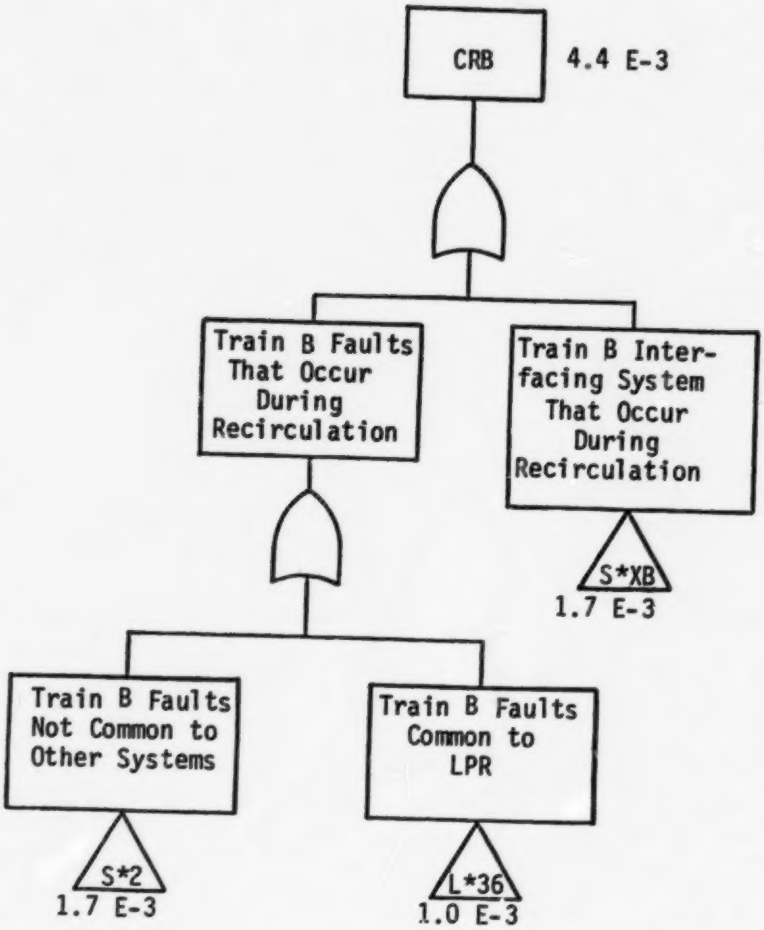

CRB
4.4 E-3
Train B Faults That Occur During Recirculation
Train B Inter-facing System That Occur During Recirculation
S*XB
1.7 E-3
Train B Faults Not Common to Other Systems
S*2
1.7 E-3
Train B Faults Common to LPR
L*36
1.0 E-3

Figure M.10 Modularized Fault Tree for Event "CRB"

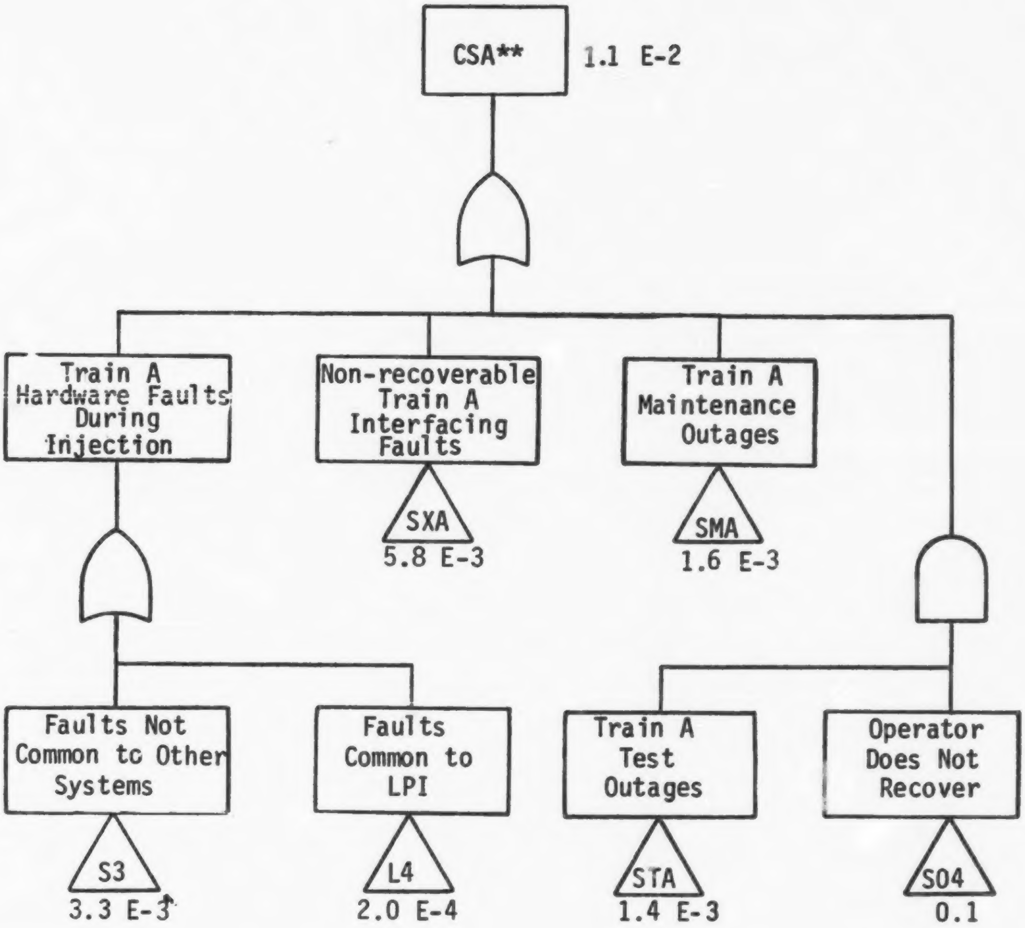

CSA**
1.1 E-2
Train A Hardware Faults During Injection
Non-recoverable Train A Interfacing Faults
SXA
5.8 E-3
Train A Maintenance Outages
SMA
1.6 E-3
Faults Not Common to Other Systems
S3
3.3 E-3
Faults Common to LPI
L4
2.0 E-4
Train A Test Outages
STA
1.4 E-3
Operator Does Not Recover
SO4
0.1

Figure M.11 Modularized Fault Tree for Event "CSA**"

[redacted]

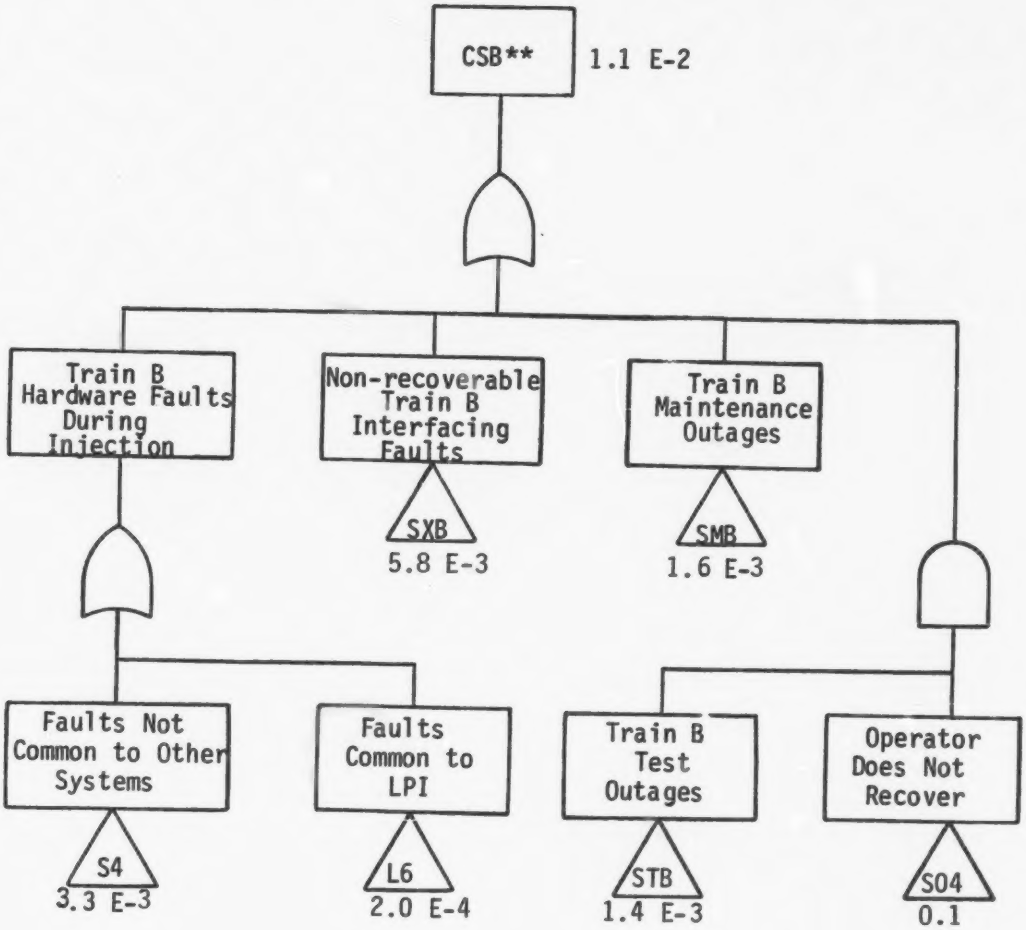

CSB**
1.1 E-2
Train B Hardware Faults During Injection
Non-recoverable Train B Interfacing Faults
SXB
5.8 E-3
Train B Maintenance Outages
SMB
1.6 E-3
Faults Not Common to Other Systems
S4
3.3 E-3
Faults Common to LPI
L6
2.0 E-4
Train B Test Outages
STB
1.4 E-3
Operator Does Not Recover
S04
0.1

Figure M.12 Modularized Fault Tree for Event "CSB**"

Table M.8 Containment Spray Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS — NOTES

CSR = L04 + S03 + CRB·CSA** + CRA·CSB** + CRA·CRB

CSA** = S3 + L4 + SXA + SMA + STA·S04

CSB** = S4 + L6 + SXB + SMB + STB·S04

INTERMEDIATE EVENTS

CRA = S*1 + S*XA + L*34

CRB = S*2 + S*XB + L*36

S*XA = DA* + ACA* 1

S*XB = DB* + ACB* 1

NOTES: 1. Offsite power is assumed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

BEST DOCUMENT AVAILABLE

Table M.9 (1/5) Event "CSR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L04	OPERATOR	FAILS TO SWITCH TO RECIRCULATION	D		3.0 E-3	$10^+, 10^-$		4
S03	OPERATOR	FAILS TO THROTTLE SPRAY VALVES	D		1.0 E-3	$10^+, 10^-$		5

Table M.9 (2/5) Event "CRA" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S*1		TRAIN A FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	PUMP BSP-1A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
	VALVE BSV-3	FAILS TO THROTTLE	D		1.0 E-3	3^+, 3^-		
	R.B. SUMP	BLOCKED			ε			
	STRAINER	PLUGGED			ε			
					Σ=1.7 E-3			
S*XA		SYSTEM INTERFACING FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	DA*	DHCCCS TRAIN A FAILS DURING RECIRCULATION			1.7 E-3			2, 3
	ACA*	AC POWER TRAIN A FAILS DURING RECIRCULATION			ε			
	DCA*	DC POWER TRAIN A FAILS DURING RECIRCULATION			ε			
L*34		TRAIN A FAULTS COMMON TO LPR			1.0 E-3			4

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.9 (3/5) Event "CRB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S*2		TRAIN B FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	PUMP BSP-1B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
	VALVE BSV-4	FAILS TO THROTTLE	D		1.0 E-3	3^+, 3^-		
	R.B. SUMP	BLOCKED			ε			
	STRAINER	PLUGGED			ε			
					Σ=1.7 E-3			
S*XB		SYSTEM INTERFACING FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	DB*	DHCCCS TRAIN B FAILS DURING RECIRCULATION			1.7 E-3			2, 3
	ACB*	AC POWER TRAIN A FAILS DURING RECIRCULATION			ε			
	DCB*	DC POWER TRAIN B FAILS DURING RECIRCULATION			ε			
L*36		TRAIN B FAULTS COMMON TO LPR			1.0 E-3			4

Table M.9 (4/5) Event "CSA**" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S3		TRAIN A FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			1
L4		TRAIN A FAULTS COMMON TO LOW PRESSURE SYSTEM			2.0 E-4			1
SXA		TRAIN A SYSTEM INTERFACING FAULTS						1,6
	DA	DHCCCS TRAIN A FAILS NON LOSP			4.3 E-2			
	ACA	AC POWER TRAIN A FAILS NON LOSP			ε			
	DCA	DC POWER TRAIN A FAILS NON LOSP			ε			
SMA		TRAIN A MAINTENANCE OUTAGE			1.6 E-3	3^+, 3^-	M	1
STA· S04		TRAIN A IN TEST AND NOT RECOVERED FOR RECIRCULATION			1.4 E-4			
	STA	TRAIN A IN TEST			1.4 E-3			
	S04	OPERATOR FAILS TO RECOVER			0.1 π=1.4 E-4	3^+, 10^-	0	

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table M.9 (5/5) Event "CSB**" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S4		TRAIN B FAULTS NOT COMMON TO OTHER SYSTEMS			1.3 E-2			1
L6		TRAIN B FAULTS COMMON TO LOW PRESSURE SYSTEM			2.0 E-4			1
SXB		TRAIN B SYSTEM INTERFACING FAULTS						1,6
	DB	DHCCCS TRAIN B FAILS						
		NON LOSP			4.3 E-2			
	ACB	AC POWER TRAIN B FAILS			ε			
	DCB	DC POWER TRAIN B FAILS			ε			
SMB		TRAIN A MAINTENANCE OUTAGE			1.6 E-3	3^+, 3^-	M	1
STB·SO4		TRAIN B IN TEST AND NOT RECOVERED FOR RECIRCULATION			1.4 E-4			1
	STB	TRAIN B IN TEST			1.4 E-3			
	SO4	OPERATOR FAILS TO RECOVER			0.1	3^+, 10^-	0	
					*=1.4 E-4			

Table M.9 Containment Spray Recirculation

QUANTIFICATION TABLES

NOTES

1 For definition see CSI fault tree analysis.

2 Failure of DHCCCS Train A(B) during recirculation phase implies success during injection phase.

3 For loss of offsite power initiator failure of DA(DB) due to diesel failure is assumed to be recovered for the recirculation phase.

4 See LPR fault tree analysis.

5 Operator is required to throttle valves BSV-3 and 4 to prevent pump cavitation. This was assessed as 1.0 E-3 rather than the usual value of 1.0 E-2 for operator faults because procedures are clear and fault is alarmed. Inclusion of this fault in the analysis may be conservative because it is not certain that throttling these valves is required to prevent cavitation.

6 In CSA** and CSB** for LOSP, the events SXA and SXB exclude diesel failures because offsite power is assumed to be recovered by the recirculation phase.

Table M.10 RBSR - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
S3	3.3 E-3
L4	2.0 E-4
DA	5.8 E-3
SMA	1.6 E-3
STA·S04	1.4 E-4
S4	3.3 E-3
L6	2.0 E-4
DB	5.8 E-3*
SMB	1.6 E-3
STB·S04	1.4 E-4
S*1	1.7 E-3
DA*	1.7 E-3
L*34	1.0 E-3
S*2	1.7 E-3
DB*	1.7 E-3
L*36	1.0 E-3
S04	1.0 E-1
L04	3.0 E-3
S03	1.0 E-3

APPENDIX N

REACTOR BUILDING ISOLATION SYSTEM (RBIS)

APPENDIX N REACTOR BUILDING ISOLATION SYSTEM (RBIS)

N.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the reactor building isolation system (or containment isolation system, CIS) is to insure that no path exists between the containment atmosphere and the outside environment. However, emergency system piping penetrating the containment must remain open (e.g., Emergency Core Cooling Systems, Containment Sprays, and Containment Cooling Fan System). The largest penetrations to be closed are the 48-inch reactor building purge supply and exhaust ducts.

In this analysis only the closure of the purge isolation valves was treated. All smaller penetrations and liquid flow paths were not analyzed since their contribution to offsite dose consequences would be comparatively small.

N.1.1 SYSTEM DESCRIPTION

The majority of the reactor building isolation system is passive. Most containment isolation valves are locked closed or normally closed. The valves which are not locked closed receive a signal to close from the ESAS when a pressure greater than 4 psi is detected within the containment. Only two containment penetrations are normally open. The 48-inch reactor building purge supply and purge exhaust ducts are frequently open while the reactor is at power. Two valves, one pneumatic, one motor operated, are in each line on opposite sides of the containment wall. The pneumatic valve is held open by instrument air. If air pressure or control power to the valve operator is lost, the valve will automatically close. The motor operated valve must be driven closed.

The valve operators on the 48-inch butterfly valves located outside of the reactor building are of the spring return air cylinder type with the spring driving the valve closed. Each pneumatic valve is controlled with two 3 way solenoid valves, either capable of permitting the valve to close in two seconds maximum time. These valves on the exterior of the reactor building are in areas totally protected from damage by missiles or pipe and equipment rupture.

The valve operators on the valves located on the inside of the reactor building are electric motor driven with a totally enclosed, non-ventilated type motor and gear drive. The valves close in five seconds maximum time. Both internal and external valves are capable of satisfactory performance in the post-accident ambient.

The system has interfaces with the ESAS reactor building isolation and cooling circuits, radiation detection circuits and 480VAC from ES MCC 3A1, unit 8A. The ESAS and high radiation signal affect both penumatic and motor operated valves, while only the motor operated valves have an interface with the 480V AC power.

The following critical design requirements were applied to the four 48-inch purge isolation valves:

a. Exterior valves:

- Must be capable of closing against a differential pressure of 55 psig.
- Must close fully in 2 seconds.
- When closed, the valve must seal bubble-tight, that is, no air bubbles appear in a pool of water, with 63.3 psig air pressure applied across the closed face.

b. Interior Valves:

- Must be capable of closing against a differential pressure of 55 psig.
- Must close fully in 5 seconds.
- When closed, the valve must seal bubble-tight under the same conditions as above.

N.1.2 SYSTEM OPERATION

The reactor building isolation system is actuated by either the Engineered Safeguard Actuation System (ESAS), or by manual action. High radiation in the reactor purge line will close the purge valves. Upon receipt of the ESAS signal (Reactor Building Isolation and Cooling, RBIC) all system valves which are not manually operated (and locked closed) are commanded closed.

The ESAS will generate a closure signal to the valves when a reactor building pressure exceeding 4 psi is detected. A second signal, generated from a high radiation detector in the reactor building purge exhaust line, will also allow valve closure. Manual actuation from the control room is a third method for closing the valves.

It should be noted that for small LOCAs, (B4), only manual operations or operation by the radiation detection circuits is possible.

The radiation detection circuit is a single train system containing no redundancy.

N.2 SYSTEM SIMPLIFIED FAULT TREE

A detailed fault tree for the RBIS was constructed to model the failure to isolate the outside environment from containment atmosphere.

The top event was defined as:

> Containment Isolation Fails - failure of
> one or both of the containment purge
> lines to isolate.

The simplified fault tree shown in Figure N.1 was constructed from the detailed tree. The simplified tree shows only the single passive and active faults and double active faults. All higher order combinations of component faults were considered to be negligible contributors to system failure probability. Human error events are also shown on the fault tree.

MAJOR ASSUMPTIONS

The major assumptions used to construct the detailed fault tree are listed below:

(1) Penetrations less than 4 inches in diameter are not considered since flow rates having a significant effect on consequences would not be realized.

(2) Liquid flow paths and paths into liquid systems were not analyzed.

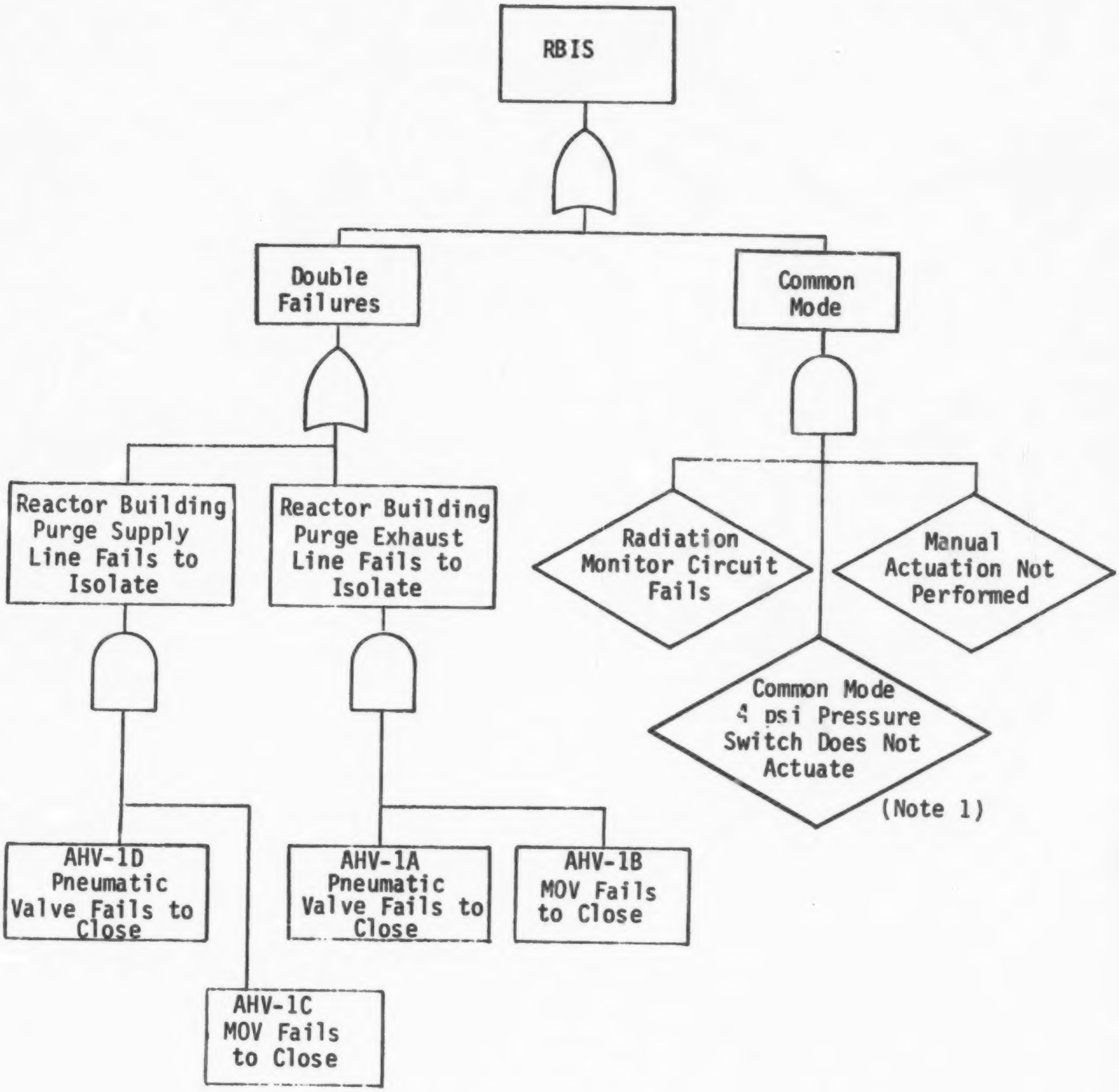
(3) Leak rate test penetrations were not analyzed due to the double passive failures required for a breach of containment isolation.

(4) The penetrations which dominate the containment leakage event are the 48-inch reactor building purge supply and exhaust lines.

(5) The containment purge supply and exhaust lines are frequently open during power operation. In this analysis the isolation valves are considered to be always open.

(6) A small LOCA, (B4), does not generate enough pressure within the containment to generate a trip (4 psig) signal from the ESAS. Therefore, only a high radiation trip or a manual actuation signal is available during a small LOCA.

(7) High radiation in the purge exhaust line was assumed to be present for all LOCA sizes.


RBIS
Double Failures
Common Mode
Reactor Building Purge Supply Line Fails to Isolate
Reactor Building Purge Exhaust Line Fails to Isolate
Radiation Monitor Circuit Fails
Manual Actuation Not Performed
Common Mode 4 psi Pressure Switch Does Not Actuate
(Note 1)
AHV-1D Pneumatic Valve Fails to Close
AHV-1A Pneumatic Valve Fails to Close
AHV-1B MOV Fails to Close
AHV-1C MOV Fails to Close

NOTES: 1. From ESAS Fault Tree

Figure N.1 Simplified Fault Tree Reactor Building Isolation System

N.3 SYSTEM QUANTIFICATION

N.3.1 SYSTEM RELIABILITY CHARACTERISTICS

For large LOCAs (B1, B2, B3) the failure to isolate the containment is determined by the failure of at least one isolation valve to close in the purge supply and in the purge exhaust line.

For small LOCAs (B4) the dominant contributor is failure to initiate containment isolation by a high radiation signal and the operator fails to manually isolate the containment. Other contributors are several orders of magnitude smaller.

N.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the RBIS failure to isolate the containment after a LOCA. Two modularized fault trees, using the simplified fault tree in Figure N.1, were constructed to accommodate different LOCA sizes. One modularized tree represents large LOCAs (B1,B2,B3) and the second represents small LOCAs (B4). The distinction is necessary since the 4 psig reactor building pressure was assumed not to be reached after a small LOCA. Therefore, only an operator action will initiate containment isolation; high radiation in the purge line will close the purge valves.

Table N.1 shows the RBIS success requirement. Table N.2 contains the top event definitions for the modularized fault tree. The modularized trees are shown in Figures N.2 and N.3. On the trees, the unavailability of each gate is shown. Table N.3 shows the Boolean equations that represent the fault trees and Table N.4 shows the quantification of each gate by component and failure mode. The point estimates for each gate are summarized in Table N.5.

Table N.1 Reactor Building Isolation System

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B1,B2,B3,B4	1/2, taken twice (at least one of two valves in each line must close)	1

NOTES

1 Both the reactor building purge supply and exhaust lines must be closed within a specified time.

Table N.2 Reactor Building Isolation System

TOP EVENT DEFINITIONS

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
CIS	Containment Isolation fails	1
CIS*	Containment Isolation fails	2

NOTES

1 CIS applies to large LOCAs (B1,B2,B3)

2 CIS* applies to small LOCAs (B4)

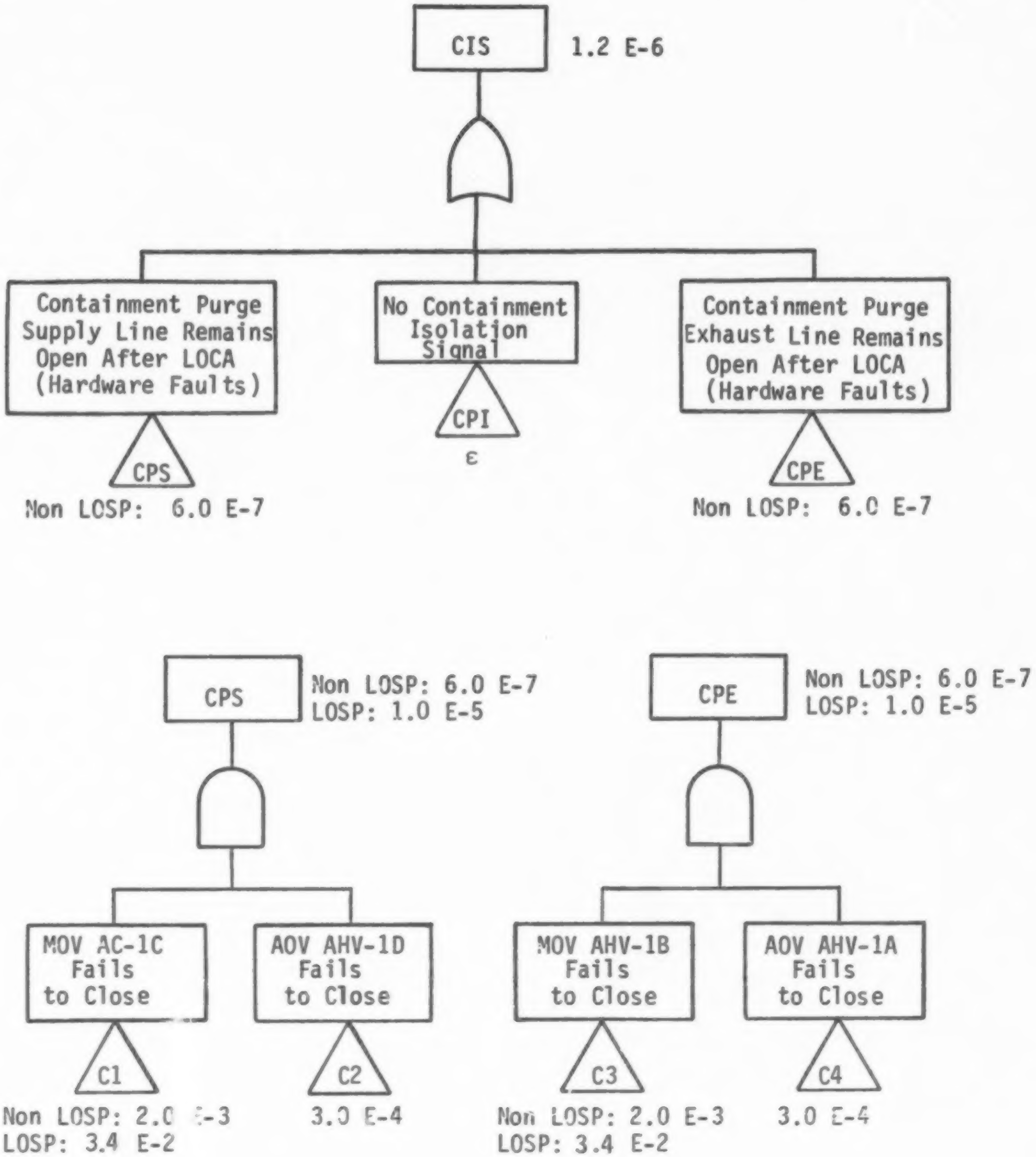

CIS
1.2 E-6
Containment Purge Supply Line Remains Open After LOCA (Hardware Faults)
CPS
Non LOSP: 6.0 E-7
No Containment Isolation Signal
CPI
ε
Containment Purge Exhaust Line Remains Open After LOCA (Hardware Faults)
CPE
Non LOSP: 6.0 E-7
CPS
Non LOSP: 6.0 E-7
LOSP: 1.0 E-5
CPE
Non LOSP: 6.0 E-7
LOSP: 1.0 E-5
MOV AC-1C Fails to Close
C1
Non LOSP: 2.0 E-3
LOSP: 3.4 E-2
AOV AHV-1D Fails to Close
C2
3.0 E-4
MOV AHV-1B Fails to Close
C3
Non LOSP: 2.0 E-3
LOSP: 3.4 E-2
AOV AHV-1A Fails to Close
C4
3.0 E-4

Figure N.2 (1/2) Modularized Fault Tree for Events "CIS", "CPS", and "CPE" (B_1, B_2, B_3 LOCAs)

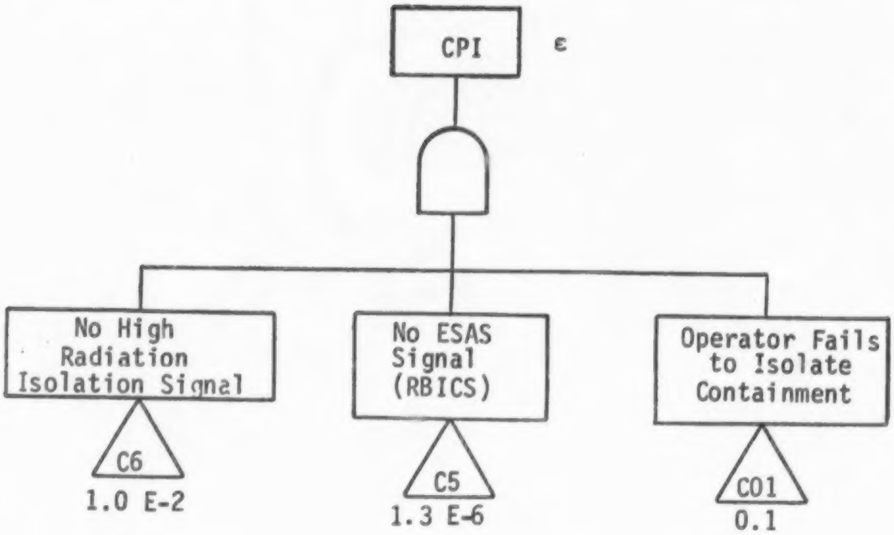

CPI
ε
No High Radiation Isolation Signal
C6
1.0 E-2
No ESAS Signal (RBICS)
C5
1.3 E-6
Operator Fails to Isolate Containment
C01
0.1

Figure N.2 (2/2) Modularized Fault Tree for Event "CPI" (B_1, B_2, B_3 LOCAs)

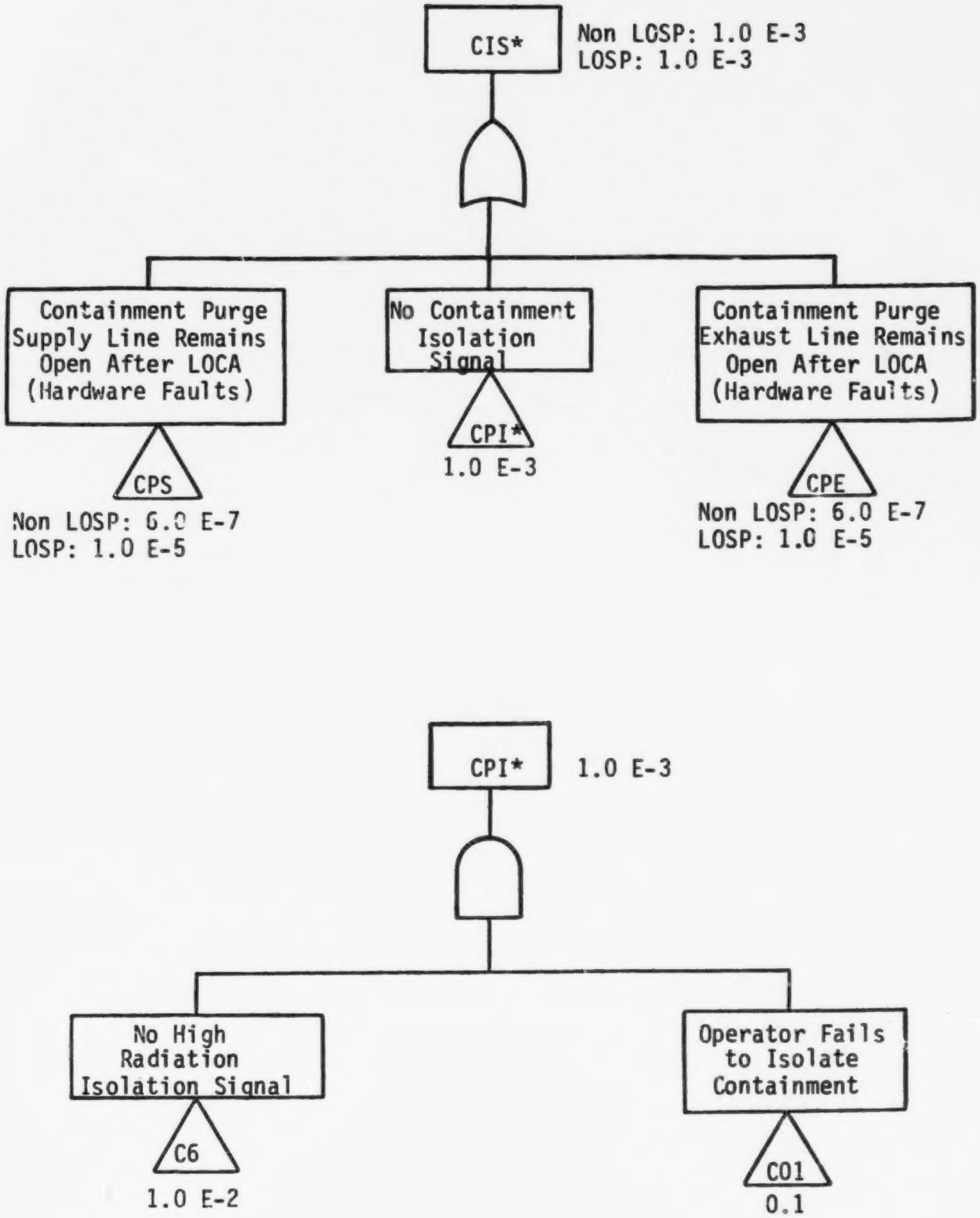

CIS*
Non LOSP: 1.0 E-3
LOSP: 1.0 E-3
Containment Purge Supply Line Remains Open After LOCA (Hardware Faults)
CPS
Non LOSP: 6.0 E-7
LOSP: 1.0 E-5
No Containment Isolation Signal
CPI*
1.0 E-3
Containment Purge Exhaust Line Remains Open After LOCA (Hardware Faults)
CPE
Non LOSP: 6.0 E-7
LOSP: 1.0 E-5
CPI*
1.0 E-3
No High Radiation Isolation Signal
C6
1.0 E-2
Operator Fails to Isolate Containment
C01
0.1

Figure N.3 (1/1) Modularized Fault Tree for Event "CIS*" and "CPI*" (B_4 LOCA)

Table N.3 Reactor Building Isolation System

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT

NOTES

B1,B2,B3 - LOCAs:

CIS = CPS + CPE + CPI

B4 - LOCAs:

CIS* = CPS + CPE + CPI*

INTERMEDIATE EVENTS

B1,B2,B3 - LOCAs:

CPI = C6·C5·C01

B4 - LOCAs:

CPI* = C6·C01

all LOCAs:

CPS = C1 · C2

CPE = C3 · C4

Table N.4 (1/4) Event "CPS" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR⁻1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPS		CONTAINMENT PURGE SUPPLY LINE REMAINS OPEN AFTER LOCA (HARDWARE FAULTS)			6.0 E-7* 1.0 E-5**			
C1		MOTOR OPERATED VALVE AHV-1C FAILS TO CLOSE			2.0 E-3* 3.4 E-2**			
	MOV AHV-1C	FAILS TO CLOSE	D		1.0 E-3	3^+, 3^-		
	CIRCUIT BKR	FAILS TO CLOSE	D		1.0 E-3	3^+, 3^-		
		AC-TRAIN A FAILS (ACA)						
		NON LOSP			ε			
		LOSP			3.2 E-2			
					Σ=2.0 E-3*			
					Σ=3.4 E-2**			
C2		AIR OPERATED VALVE AHV-1D FAILS TO CLOSE			3.0 E-4			
	AOV AHV-1D	FAILS TO CLOSE	D		3.0 E-4			
					π=6.0 E-7*			
					π=1.0 E-5**			

*NON LOSP

**LOSP

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPE		CONTAINMENT PURGE EXHAUST LINE REMAINS OPEN AFTER LOCA (HARDWARE FAULTS)			6.0 E-7* 1.0 E-5**			
C3		MOTOR OPERATED VALVE AHV-1B FAILS TO CLOSE			2.0 E-3* 3.4 E-2**			
	MOV AHV-1B	FAILS TO CLOSE	D		1.0 E-3	3^+, 3^-		
	CIRCUIT BKR	FAILS TO CLOSE	D		1.0 E-3	3^+, 3^-		
		AC-TRAIN A FAILS (ACB)						
		NON LOSP			ε			
		LOSP			3.2 E-2			
					Σ=2.0 E-3*			
					Σ=3.4 E-2**			
C4		AIR OPERATED VALVE AHV-1A FAILS TO CLOSE			3.0 E-4			
	AOV AHV-1A	FAILS TO CLOSE	D		3.0 E-4			
					π=6.0 E-7*			
					π=1.0 E-5**			

*NON LOSP

**LOSP

Table N.4 (2/4) Event "CPE" Quantification

Table N.4 (3/4) Event "CPI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPI		NO CONTAINMENT ISOLATION SIGNAL			1.3 E-9			
C5	ESAS (ILB4)	NO REACTOR BUILDING ISOLATION AND COOLING SYSTEM (RBICS) ISOLATION SIGNAL (SEE ESAS)			1.3 E-6			
C6		NO HIGH RADIATION SIGNAL			1.0 E-2			
	RADIATION MONITOR	FAILS			1.0 E-4	3^+, 3^-		
	COMPARATOR	OPERATOR MISCALIBRATES	D		1.0 E-2	3^+, 3^-		
					Σ=1.0 E-2			
C01		OPERATOR FAILS TO ISOLATE CONTAINMENT WHEN REQUIRED	D		0.1	3^+, 10^-	0	
					*=1.3 E-9			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table N.4 (4/4) Event "CPI*" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPI*		NO CONTAINMENT ISOLATION SIGNAL			1.0 E-3			
C6		SEE CPI QUANTIFICATION TABLE			1.0 E-2			
C01		SEE CPI QUANTIFICATION TABLE			0.1			
					π=1.0 E-3			

Table N.5 RBIS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
C1	2.0 E-3* 3.4 E-2**
C2	3.0 E-4
C3	2.0 E-3* 3.4 E-2**
C4	3.0 E-4
C5	1.3 E-6
C6	1.0 E-2
C01	0.1

*Offsite power available
**Offsite power not available

[redacted]

APPENDIX P

EMERGENCY FEEDWATER SYSTEM (EFS)

APPENDIX P EMERGENCY FEEDWATER SYSTEM (EFS)

P.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the Crystal River Emergency Feedwater System (EFS) is to backup the Main Feedwater System (MFS) in removing post shutdown decay heat from the reactor coolant system via the steam generators. During normal shutdowns the MFS is throttled down to a level capable of removing decay heat and the EFS is not utilized. However, if the plant shutdown is caused by a loss of the MFS or if the MFS is lost subsequent to the plant shutdown, then the EFS is put into operation. It is important to note that only in the B&W PWR design is it possible for the MFS to throttle down and remain on line for all shutdowns except those caused by failures in the MFS. Other PWR designs trip the MFS whenever the turbine trips before the reactor, placing the "auxiliary" feedwater system (their backup system) into operation in the majority of shutdowns. This explains why the backup feedwater system at Crystal River is labeled emergency rather than auxiliary.

P.1.1 SYSTEM DESCRIPTION

A diagram of the Crystal River Unit 3 EFS is presented in Figure P.1. The system consists of two interconnected trains, each capable of supplying emergency feedwater to either or both steam generators under automatic or manual initiation and control.

WATER SOURCES

The primary water source for both trains of the Crystal River EFS is the Condensate Storage tank, CDT-1. Water is provided to the pumps through six-inch branch lines which are fed from CDT-1 by a common eight-inch line. Each six-inch branch line contains a normally open AC-powered valve and the common eight-inch line contains a locked-open manual valve.

A reserve of 150,000 gallons is maintained within the tank and is verified by control room indication of level, control room annunciation on low level, and Technical Specification requirements.

An alternate, non-seismic qualified source of water is available for EFS use from the main condenser hotwell. Water is provided to the pumps through eight-inch branch lines which are fed from the hotwell by a common eight-inch line. Each eight-inch branch line contains a normally-closed DC-powered valve and the common eight-inch line contains a normally-open manual valve. The DC-powered valves are interlocked such that they can be opened only if at least one of the two DC-powered vacuum breaker valves is open.

PUMPS AND DISCHARGE CROSS-TIES

The pumps in both trains are Ingersol-Rand centrifugal horizontal split multi-stage type and are each rated at 740 gpm with a design recirculation flow rate of 20 gpm. Thus each pump is capable of delivering 720 gpm against maximum OTSG pressure to the discharge piping supplying both steam generators.

The Train A pump (EFP-2) is turbine-driven, capable of receiving motive steam from either OTSG or from the auxiliary steam supply from fossil-powered Units 1 and 2. The Train B pump (EFP-1) is motor-driven, powered from diesel-backed ES bus 3A.

The pumps are interconnected at their discharge by separate cross-ties, each containing a normally open DC-powered valve and a check valve. In addition, there is another cross-tie containing two normally closed manual valves.

FLOW CONTROL VALVES

The flow of emergency feedwater to steam generator A (B) is controlled by pneumatic valve FWV-40 (FWV-39). During automatic EFS initiation and control, this valve is under control of the Integrated Control System (ICS) via electric to pneumatic converters. Control for this valve, including manual control, will be described in greater detail in the Instrument and Control section.

Valve FWV-40 (FWV-39) functions both as the emergency feedwater flow control valve and as the startup feedwater flow control valve. During low power operation, flow from the main feedwater pump passes through FWV-41 (FWV-42), is controlled by FWV-40 (FWV-39), and returns to the main feedwater header through FWV-36 (FWV-33); FWV-35 (FWV-34) is closed to prevent this flow from entering the emergency feedwater nozzles.

STEAM SUPPLY FOR EFP-2

Steam for the turbine-driven pump (EFP-2) is extracted immediately downstream of both steam generators. This steam must pass through a normally-open DC-operated stop-check valve (MSV-55 or 56), a check valve (MSV-186 or 187), and a normally closed DC-operated stop valve (ASV-5). Initiation of the turbine-driven pump is accomplished by opening this stop valve. Initiation signals are described in the Instrument and Control section.

In addition, an alternate source of steam is available from fossil-powered Units 1 and 2 which connect immediately upstream of ASV-5. Lineup of this source requires local, manual operation of valves at Unit 3.

OTHER SYSTEM FEATURES

The primary components for EFS operation following a loss of the main feedwater system are described above. There are additional system features, however, which affect overall system performance. These features are described below:

> Steam Line Rupture Matrix: This feature is a redundant Class IE logic matrix that senses low steam generator pressure and isolates the generator with low pressure by closing main steam isolation valves, main feedwater isolation valves and emergency feedwater isolation valves FWV-35, 36, and 162 for SG-A or FWV-33, 34, and 161 for SG-B.

Remote Manual Bypass Valves: A Remote-manual, normally open, DC powered bypass valve is provided in each EFS supply line to the steam generators (FWV-162 for SG-A and FWV-161 for SG-B). These valves provide a back-up means of controlling EFS flow should the ICS-controlled valves (FWV-40, 39) fail for any reason. They are pre-throttled to provide approximately 550 gpm to each steam generator at design pressure.

VALVE INDICATIONS AND OPERABILITY

All AC- and DC-powered valves fail "as is" on the loss of electric power. All such valves shown in Figure P.1 are controllable from the control room and their position is indicated in the control room. Power for the indication and control of these valves is derived from the power source for the respective valve motors. Only four valves (EFV-4 and 8 for SG-A and EFV-3 and 7 for SG-B)are AC-powered (non-vital) and they are normally open.

The pneumatic flow control valves (FWV-40, 39) will fail "as is" on loss of supply air pressure. An air lock is provided that senses low air pressure and de-energizes a solenoid valve to lock the existing air pressures across the control valve piston. An air reservoir is provided for each valve which allows remote-manual opening of the control valve when normal supply air is lost. This is accomplished using DC-powered solenoid valves to direct air from the reservoir to the underside of the control valve piston while venting the top of the piston. Loss of power to the electric/pneumatic converters will result in the valves assuming a position of approximately half-open.

In addition to the backup air supply, further reliability is achieved by the provision of remote-manual DC-powered valves (FWV-162, 161).

SYSTEM INTERFACES

Cooling Systems

Cooling water for the EFS pumps is required for successful operation of the EFS. At the time the analysis was performed, both pumps were cooled by water provided by the Nuclear Services Closed Cycle Cooling System (NSCCCS), which thus creates an undesirable AC-power dependency for this system. Florida Power Corp. had recognized this dependency and proposed to eliminate it by modifying the pump cooling design to make both pumps self cooled.* For this reason, the analysis herein assumes the EFS pumps are self-cooled.

The pumps are separated by a missile wall and are located in the intermediate building. The intermediate building is cooled by two 100% air fan subsystems. The main steam lines also run through this building at an elevation above the pumps. Missile protection is provided by internal building structure but the pumps and steam lines are in air communication.

Lubricating System

Lubricating oil for the EFS pumps is an integral system powered by the pump shaft, and requires no electrical input.

Electric Power Systems

Simplified diagrams showing power distribution for the EFS are shown in Figures P.2 through P.4. The motor-driven emergency feedwater pump (EFP-1) AC power interface is shown in Figure P.2. EFS automatic start control circuit power dependencies are shown in Figure P.3. It can be noted from Figure P.5 that DC power is required to close the breaker for the motor-driven pump. DC-powered EFS valves are powered as shown in Figure P.3. AC-powered valves (EPV-3, 4, 7, and 8) are not diesel backed and are powered as shown in Figure P.4; these valves are normally open and fail "as is" on loss of power. Flow paths from each pump to both steam generators are available without any valve repositioning.

---

*FPC has indicated that both the turbine-driven and electric-driven pumps will be modified. It is noted, however, that only the modification to the turbine-driven pump will cause a significant improvement in predicted system reliability.

In the event of loss of main feedwater induced by loss of offsite power, the motor-driven EFS pump (EFP-1) will not start automatically; it must be manually loaded on the diesel. Loss of offsite power will also result in a loss of normal air supplies but backup is available as previously described. The follow up action in the plant operating procedure for loss of offsite power requires manual loading of air compressors on the diesels.

In the event of a total loss of AC power (offsite and diesels), the EFS flow will be initiated through the DC-powered steam supply valve and the turbine driven pump.

INSTRUMENTATION AND CONTROL

Initiation Logic

A simplified diagram of EFS initiation is shown in Figure P.5. This diagram is functional in nature and does not represent actual hardware. The actual logic is contained in relay racks and the individual component controllers. Automatic initiation will occur whenever one of two conditions exists: loss of both main feedwater pumps or low level in both steam generators. The non-redundant single train logic in the relay cabinets de-energizes a relay to initiate the EFS. A loss of the vital 120VAC source powering these cabinets will also cause initiation. The automatic initiation will open ASV-5 and MSV-55 (MSV-55 and 56 are normally open) to start the turbine-driven pump. The initiation signal also causes the circuit breaker to start the motor-driven pump provided the two interlocks described below are satisfied. Once a pump is started, EFS flow will exist since the flowpaths, including the discharge cross-connects, are normally open.

In addition, the motor-driven pump is interlocked to prevent automatic start unless offsite power is available on the ES bus and one of the suction valves (EFV-2 or 3) is open.

A key-operated bypass is provided to prevent inadvertent initiation of the EFS when the main feedwater pumps are secured during normal startups and shutdowns. This bypass feature does not have automatic removal but it is under administrative control. Initiation on low steam generator level is provided as a backup means of ensuring EFS initiation and this actuation feature is not bypassed.

Flow Control

Normal control of EFS flow is achieved with flow control valves FWV-39 and 40. The ICS senses the loss of main feed pumps or low level in the steam generators and opens the EFS Block Valves (FWV-34 and 35) and closes the Main Feedwater Connections (FWV-33 and 36). This directs EFS flow through FWV-39 and 40 to the upper nozzles in the steam generators.

FWV-39 and 40 are pneumatic-operated valves and are normally controlled by the ICS via electric/pneumatic converters. The ICS adjusts these valves to attain and maintain one of two steam generator level setpoints, depending on reactor coolant pump (RCP) status. If the RCP's are running, the low level is maintained. If the RCP's are off, the high setpoint is maintained in order to promote natural circulation in the reactor coolant system. A loss of the ICS control signal will result in the valve failing to a position approximately 50% open. On loss of supply air pressure, the valve will fail "as is", which, depending on SG level at the time of failure, could be the closed position. *

In addition to the backup provisions for FWV-39 and 40, DC-powered bypass valves (FWV-161 and FWV-162) are provided. These valves are prethrottled to allow a flow rate of approximately 550 gpm to each steam generator, to ensure flow is established should FWV-34, 35, 39, or 40 fail. Once EFS initiation occurs, the operator will verify proper operation of the normal flow control path and then close FWV-161 and 162. Failure to close these valves could result in a rapid cool down transient.

---

*However, each valve has associated with it an air accumulator allowing for 2-3 full valve strokes.

Instrumentation

The availability of several important instrument indicators in the control room for three specific incident initiators is tabulated below:

Indication	Loss of MFW	Loss of MFW Due to Loss of Offsite Power	Loss of All AC Power
CDT-1 level	Yes	No	No
CDT-1 level alarms	Yes	Yes	Yes
EFW flow	Yes	Yes	Yes
Valve positions	Yes	Yes*	Yes*
OTSG level	Yes	Yes	Yes
OTSG level alarms	Yes	Yes	Yes

---

*for all except AC-powered valves ESW-3, 4, 7, 8

Steam Line Rupture Matrix

Operation of the EFS can be affected by the steam line rupture matrix (SLRM).

The SLRM detects low steam pressure in either steam generator and will isolate a generator if a low pressure condition exists; low pressure must be detected by two pressure switches, one set at 725 psig, the other at 600 psig (see Figure P.6). The isolation signal will cause closure of the main steam isolation valves, main feedwater isolation valves, and emergency feedwater isolation valves for the affected steam generator.

The SLRM is a safety-grade system provided with battery-backed power and coincidence logic in the actuation circuitry. Inadvertent actuation of the SLRM could cause isolation of one steam generator.

OPERATOR ACTIONS

For a loss of MFW, no operator action is required to establish EFS flow. The operator will verify proper flow control and adjust FWV-161 and 162 as required. Certain failures (e.g., mispositioned valves, pump fail to auto start, etc.) have the potential of being corrected from the control room.

The only significant differences for a loss of MFW induced by loss of offsite power are as follows:

a. The motor-driven pump must be manually loaded onto the ES bus (from the control room).

b. Failure involving AC-powered valves EFW-3, 4, 7, or 8 would require local manual correction since they are not attached to an emergency bus.

In the event of total loss of AC power, the turbine-driven pump would start automatically and all the DC-powered valves would be operable from the control room.

Testing

The ability of either of the two pumps to deliver a minimum of 550 gpm to either steam generator with the reactor at power is verified every eighteen months (Procedure PT-123). The ability of both pumps to start automatically upon receiving the actuation signals is verified during hot shutdown every eighteen months (Procedure PT-122). Both procedures verify that the EFS can be controlled independent of the ICS. Additional automatic actuation is also verified during cold shutdown at which time automatic valve actuations by the ICS are tested (Procedure SP-416).

EFS valves are cycled once each quarter. After cycling they are verified to be in the correct position by two independent valve lineup checks. Valves with position indication in the control room are verified to be in the correct position daily. A monthly operability check of each pump is performed using the normal recirculation flow paths (Procedures SP-349 and SP-350). These checks, made on a staggered schedule for the two pumps, confirm the pumps cabability to produce the required pump discharge pressure. These checks require closure of the associated stop-check valve (EFV-7 or EFV-8). Following the tests, proper valve lineup is ensured by two independent checks.

Maintenance

Maintenance acts which require isolation of one component in the EFS occur about every quarter. The EFS has 14 active components (AOV's, MOV's, pumps) capable of being isolated without violating technical specifications (e.g., isolation of EFV-3, EFV-4, MSV-55, MSV-56, FWV-39, or FWV-40 would violate technical specifications). Isolation is achieved by closing the appropriate upstream and downstream valves from the component under maintenance.

Technical Specification Limitations

The limiting condition for operation of the EFS requires that two independent emergency feedwater pumps and associated flow paths be operable with:

a. One emergency feedwater pump capable of being powered from an operable emergency bus.

b. One emergency feedwater pump capable of being powered from an operable steam supply system.

If one emergency feedwater system becomes inoperable, it must be restored to an operable condition within 72 hours or the plant must be placed in hot shutdown within the next 12 hours.

The technical specifications also require the availability of 150,000 gallons of water in the condensate storage tank (CDT-1) for EFS use.

P.1.2 SYSTEM OPERATION

The simplified schematic of the EFS presented in Figure P.1 shows that the EFS is a two train system with a steam driven turbine pump train and an electric pump train. The pump trains draw water from either the condensate storage tank (preferred) or from the condenser hotwells and deliver to the steam generators. Either pump can feed either steam generator through interties at the pumps' discharge. Steam required to operate the turbine pump is extracted from either steam generator upstream of the four main steam isolation stop valves.

Both pump trains are started automatically following all loss of MFW events which do not involve offsite power. The pumps may also be started manually from the control room. For loss of offsite power cases, the turbine pump train starts automatically but the electric pump is started manually from the control room. Successful operation of the EFS requires full flow from one pump to the secondary side of either steam generator and discharge of the generated steam to either the condenser or atmosphere. It is also required that either forced or natural circulation be maintained on the primary side of the steam generator receiving the EFS cooling. If this is not established, the decay heat produced by the reactor will not be transmitted to the secondary side of the steam generators.

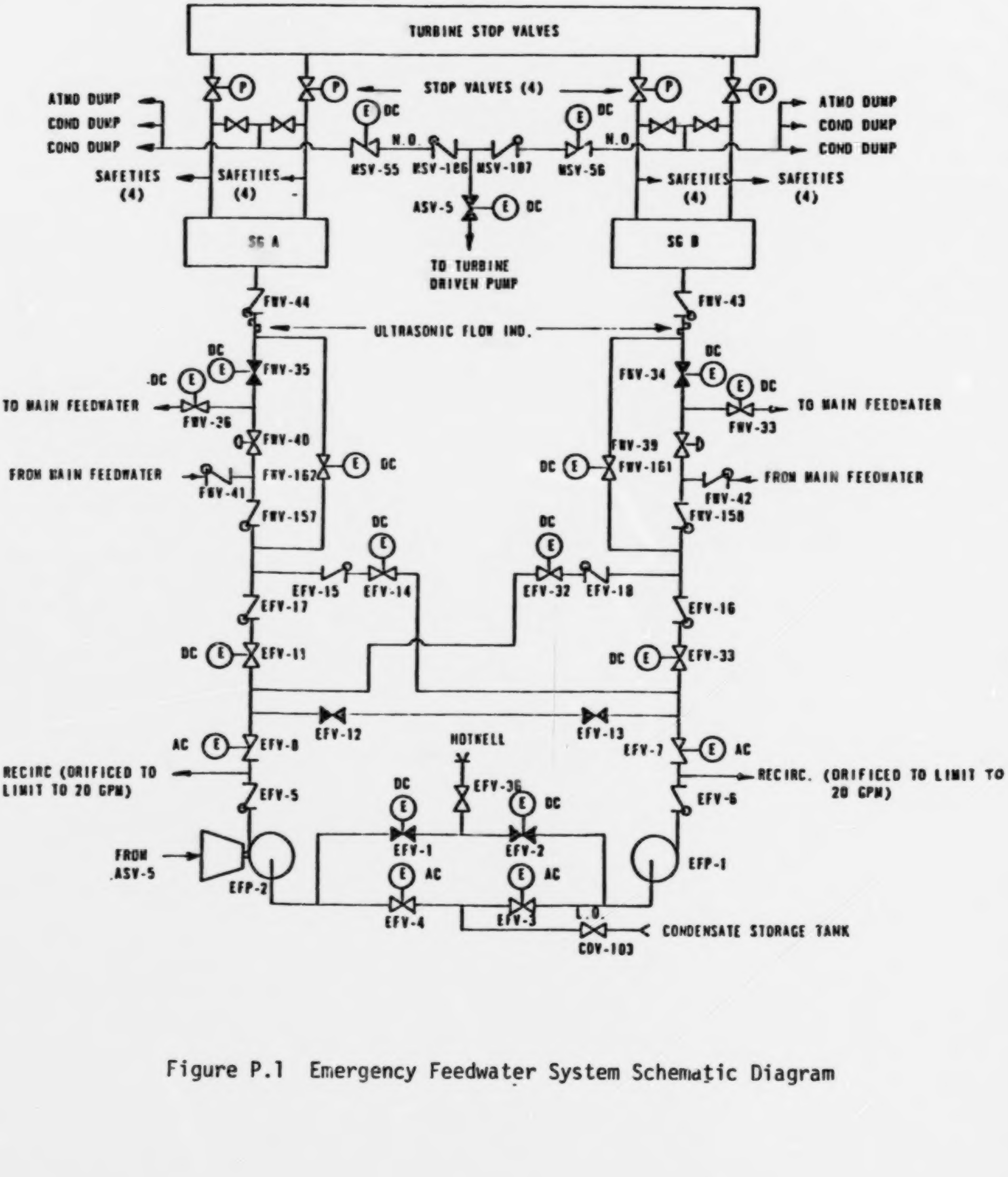
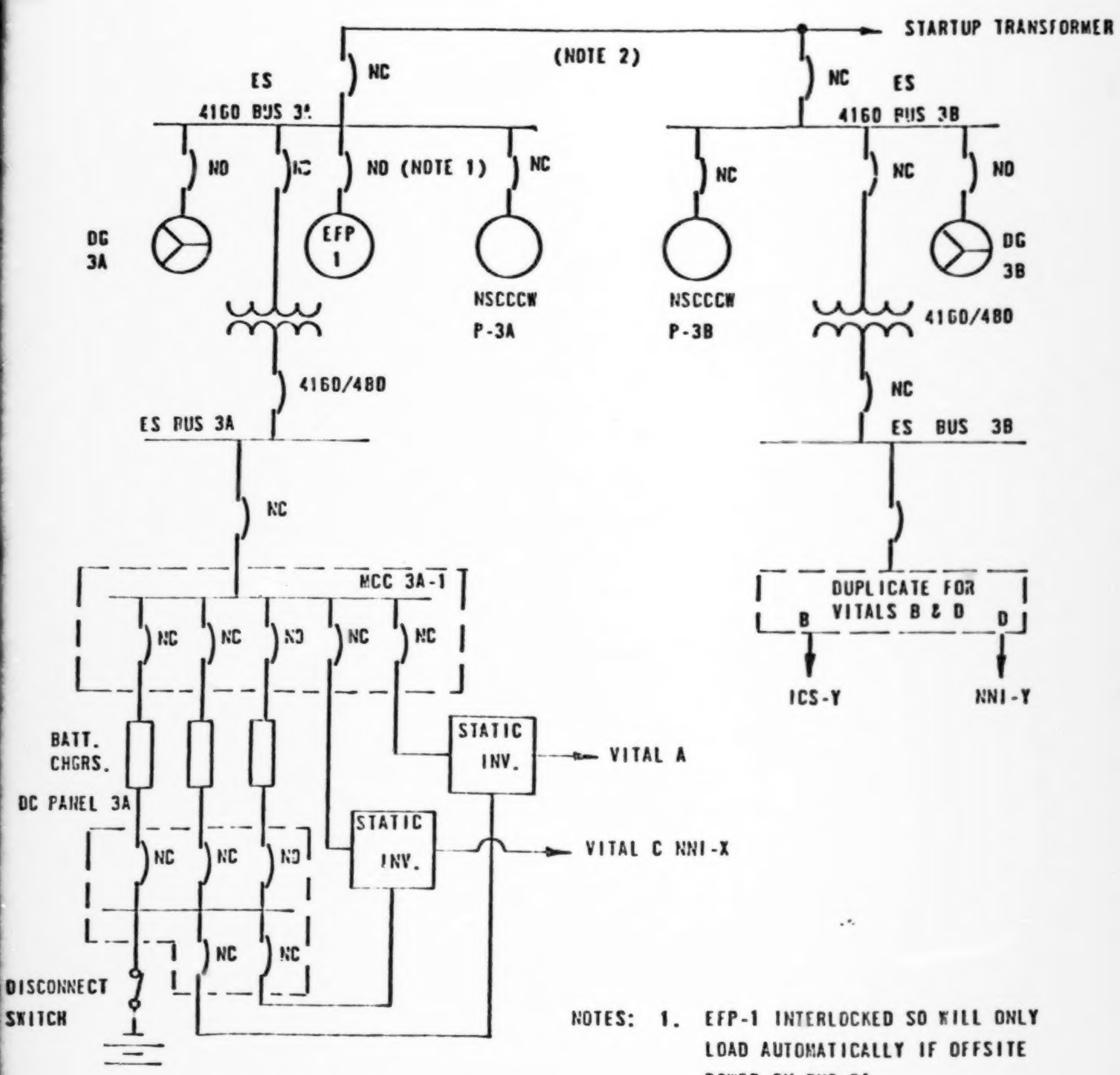

TURBINE STOP VALVES
STOP VALVES (4)
ATMO DUMP
COND DUMP
COND DUMP
ATMO DUMP
COND DUMP
COND DUMP
P
E DC
N.O.
MSV-55
MSV-106
MSV-107
MSV-56
SAFETIES (4)
SAFETIES (4)
SAFETIES (4)
SAFETIES (4)
ASV-5
E DC
TO TURBINE DRIVEN PUMP
SG A
SG B
FWV-44
FWV-43
ULTRASONIC FLOW IND.
DC
FWV-35
FWV-34
TO MAIN FEEDWATER
FWV-36
FWV-33
TO MAIN FEEDWATER
FWV-40
FWV-39
FWV-162
FWV-161
FROM MAIN FEEDWATER
FWV-41
FWV-42
FROM MAIN FEEDWATER
FWV-157
FWV-158
EFV-15
EFV-14
EFV-32
EFV-18
EFV-17
EFV-16
EFV-11
EFV-33
EFV-12
EFV-13
HOTWELL
AC
EFV-8
EFV-7
RECIRC (ORIFICED TO LIMIT TO 20 GPM)
RECIRC. (ORIFICED TO LIMIT TO 20 GPM)
EFV-5
EFV-6
EFV-36
EFV-1
EFV-2
FROM ASV-5
EFP-2
EFP-1
EFV-4
EFV-3
L.O.
CDV-103
CONDENSATE STORAGE TANK

Figure P.1 Emergency Feedwater System Schematic Diagram


STARTUP TRANSFORMER
(NOTE 2)
NC
ES
4160 BUS 3A
NC
ES
4160 BUS 3B
NO
NC
NO (NOTE 1)
NC
NC
NC
NO
DG
3A
EFP
1
NSCCCW
P-3A
NSCCCW
P-3B
DG
3B
4160/480
4160/480
NC
ES BUS 3A
ES BUS 3B
NC
MCC 3A-1
DUPLICATE FOR
VITALS B & D
B
D
ICS-Y
NNI-Y
NC
NC
NO
NC
NC
BATT.
CHGRS.
STATIC
INV.
VITAL A
DC PANEL 3A
STATIC
INV.
VITAL C NNI-X
NC
NC
NO
NC
NC
DISCONNECT
SWITCH

NOTES: 1. EFP-1 INTERLOCKED SO WILL ONLY LOAD AUTOMATICALLY IF OFFSITE POWER ON BUS 3A.

2. TWO ALTERNATE SOURCES AVAILABLE MANUALLY; UNIT 1/2 STARTUP XFMR WITHIN MINUTES AND UNIT 3 AUX. XFMR WITHIN EIGHT HOURS.

Figure P.2 Simplified Power Source Diagram

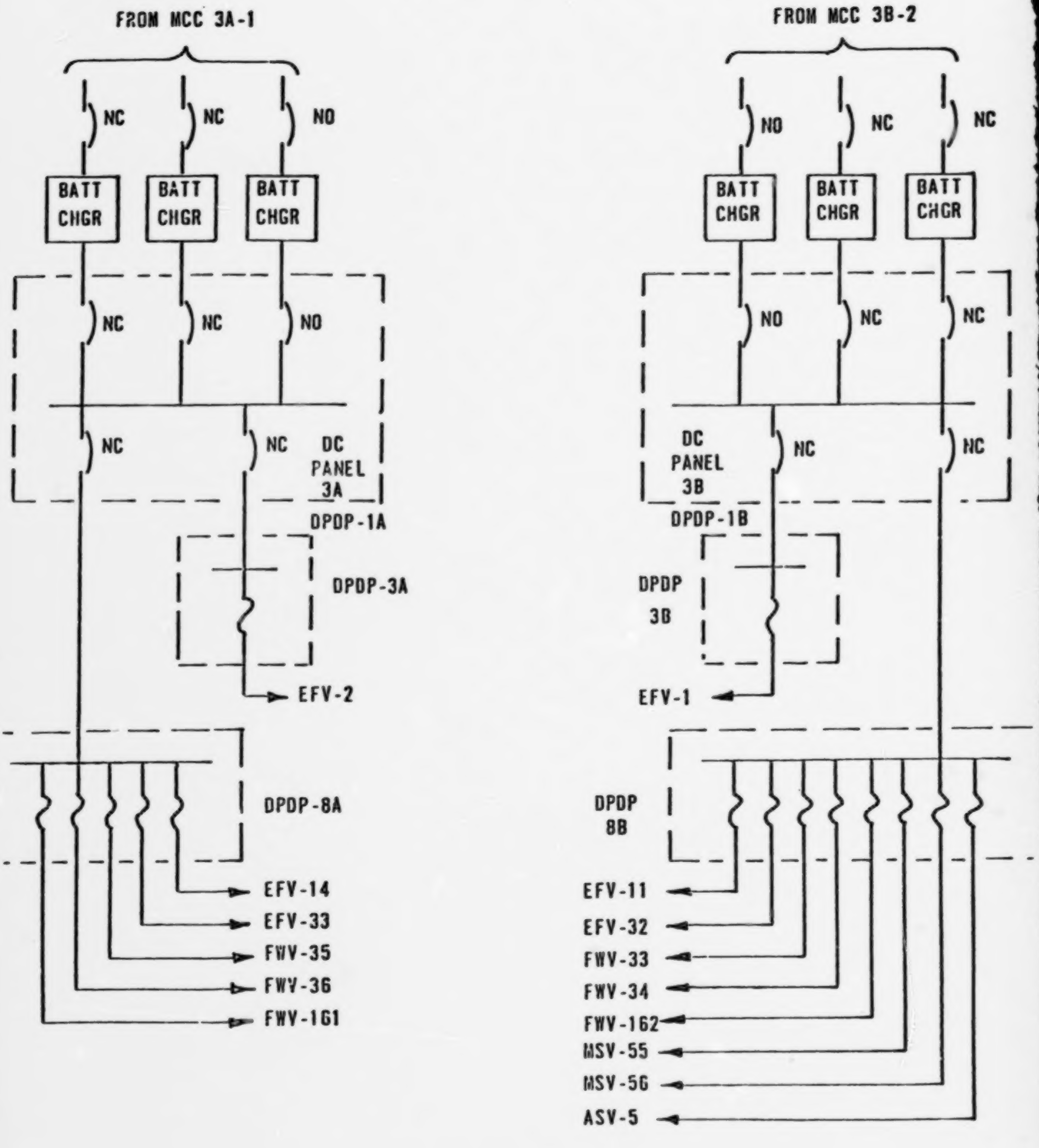

FROM MCC 3A-1
NC
NC
NO
BATT CHGR
BATT CHGR
BATT CHGR
NC
NC
NO
NC
NC
DC PANEL 3A
DPDP-1A
DPDP-3A
EFV-2
DPDP-8A
EFV-14
EFV-33
FWV-35
FWV-36
FWV-161
FROM MCC 3B-2
NO
NC
NC
BATT CHGR
BATT CHGR
BATT CHGR
NO
NC
NC
DC PANEL 3B
NC
NC
DPDP-1B
DPDP 3B
EFV-1
DPDP 8B
EFV-11
EFV-32
FWV-33
FWV-34
FWV-162
MSV-55
MSV-56
ASV-5

Figure P.3 Simplified Power Source Diagram
DC Loads

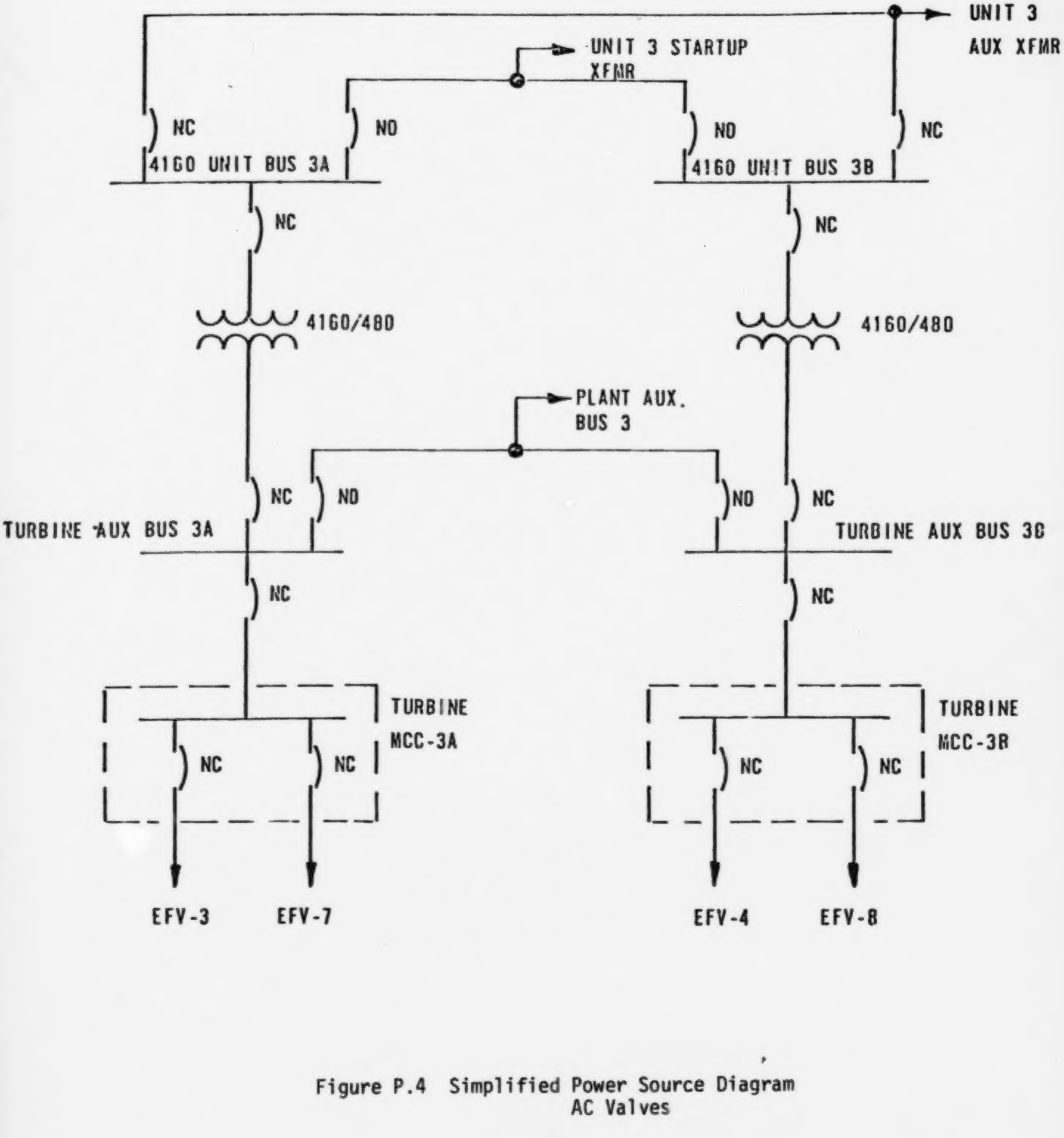

UNIT 3
AUX XFMR
UNIT 3 STARTUP
XFMR
NC
NO
NO
NC
4160 UNIT BUS 3A
4160 UNIT BUS 3B
NC
NC
4160/480
4160/480
PLANT AUX.
BUS 3
NC
NO
NO
NC
TURBINE AUX BUS 3A
TURBINE AUX BUS 3B
NC
NC
TURBINE
MCC-3A
TURBINE
MCC-3B
NC
NC
NC
NC
EFV-3
EFV-7
EFV-4
EFV-8

Figure P.4 Simplified Power Source Diagram
AC Valves

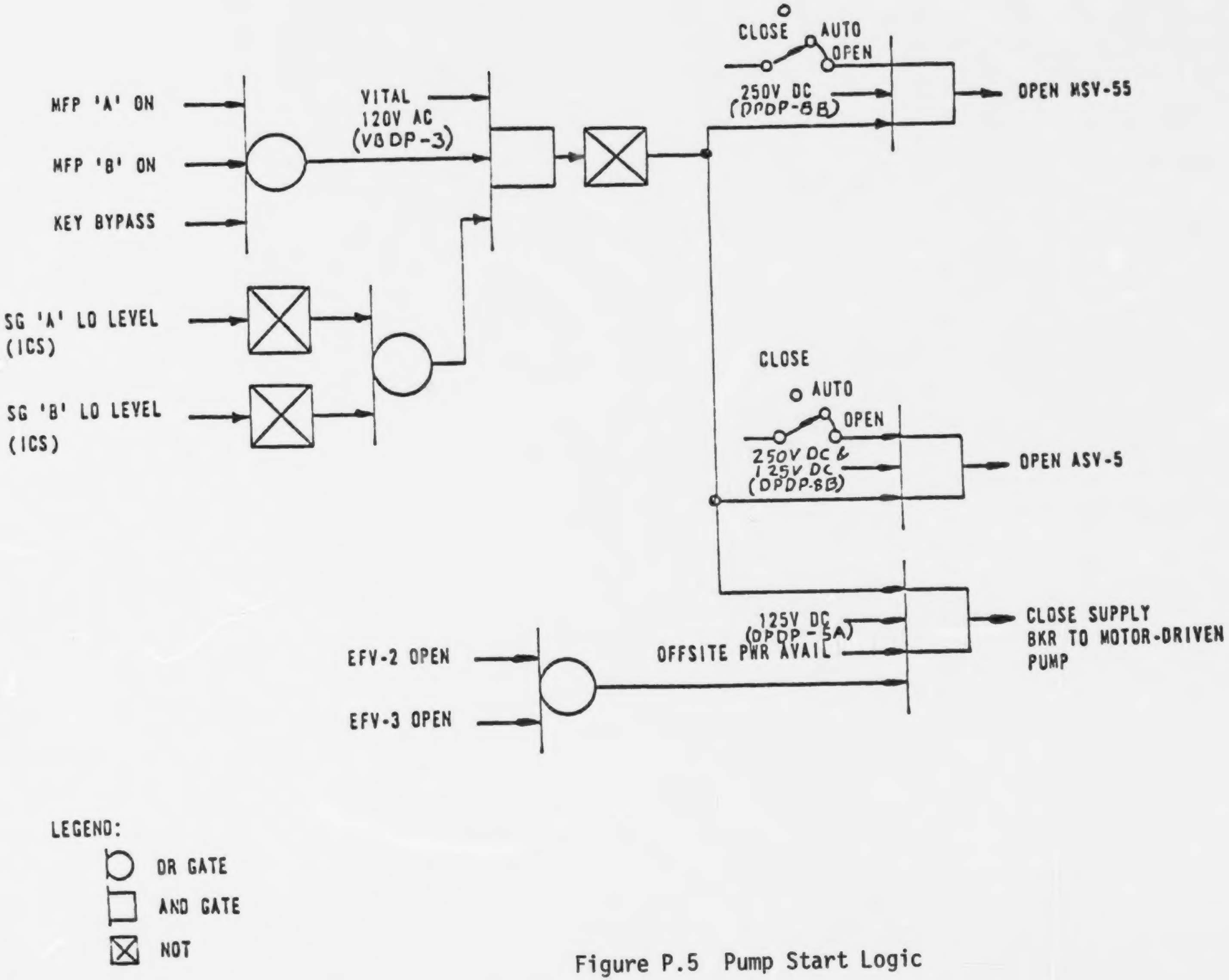
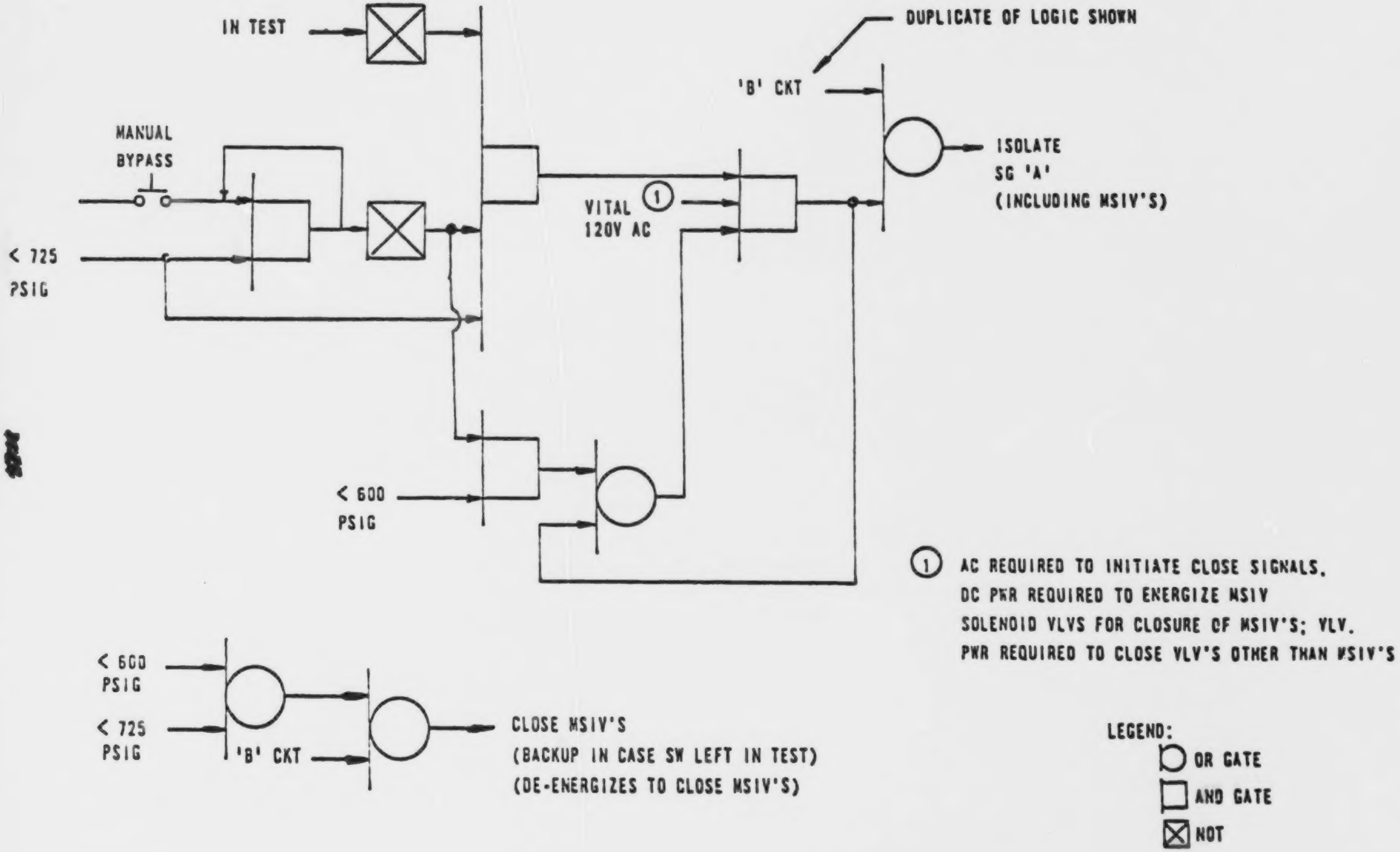

MFP 'A' ON
MFP 'B' ON
KEY BYPASS
VITAL 120V AC (VBDP-3)
SG 'A' LO LEVEL (ICS)
SG 'B' LO LEVEL (ICS)
CLOSE
AUTO
OPEN
250V DC (DPDP-8B)
OPEN MSV-55
CLOSE
AUTO
OPEN
250V DC & 125V DC (DPDP-8B)
OPEN ASV-5
125V DC (DPDP-5A)
OFFSITE PWR AVAIL
CLOSE SUPPLY BKR TO MOTOR-DRIVEN PUMP
EFV-2 OPEN
EFV-3 OPEN
LEGEND:
OR GATE
AND GATE
NOT

Figure P.5 Pump Start Logic


IN TEST
DUPLICATE OF LOGIC SHOWN
'B' CKT
MANUAL
BYPASS
ISOLATE
SG 'A'
(INCLUDING MSIV'S)
VITAL ①
120V AC
< 725
PSIG
< 600
PSIG
< 600
PSIG
< 725
PSIG
'B' CKT
CLOSE MSIV'S
(BACKUP IN CASE SW LEFT IN TEST)
(DE-ENERGIZES TO CLOSE MSIV'S)
LEGEND:
OR GATE
AND GATE
NOT

① AC REQUIRED TO INITIATE CLOSE SIGNALS. DC PWR REQUIRED TO ENERGIZE MSIV SOLENOID VLVS FOR CLOSURE OF MSIV'S; VLV. PWR REQUIRED TO CLOSE VLV'S OTHER THAN MSIV'S

Figure P.6 SLRM Logic ("A" Circuit Shown)

P.2 SYSTEM SIMPLIFIED FAULT TREE

The top event representing the failure definition is "EFS Fails to Remove Reactor Coolant System Decay Heat Via One of Two Steam Generators". EFS failure therefore occurs if both pump trains do not provide adequate flow (550 gpm initially) to the secondary side of either steam generator. The simplified EFS fault tree is presented in Figure P.7.

MAJOR ASSUMPTIONS

The assumptions made during the development of the EFS simplified fault tree include:

1. Component outages due to maintenance are considered on active components only.
2. Component outages due to test are generally negligible. All active valves are cycled quarterly and the test duration is short enough to cause a negligible outage. However, during monthly tests of the pumps, valves EFV-7 and EFV-8 are closed for a much longer period and the test outage was therefore considered.
3. No common mode coupling was assumed between valves which have open and closed status indication in the control room. All of these valves undergo a status check by the operators at least once per shift. Common mode coupling was considered between certain groups of manual valves however.
4. Although separate control circuits are provided within the ICS to control the flow of EFS to either of the steam generators, the ICS was assumed to consist of only a single control device with signals to both EFS trains. This approach was taken due to the complexity of the ICS and the time limitations imposed on this study.
5. Credit was given for an alternate water source from the hotwell should suction be lost from the condensate storage tank (see also quantification tables).

6. Although an alternate source of steam is available to the turbine-driven pump from fossil-powered Units 1 and 2, this was not considered in the analysis. Use of this steam requires operation of manual valves in Unit 3.

7. Intermediate building cooling is not important to the operation of the EFS pumps since the large building would probably heat up relatively slowly if cooling was lost. Also, the electric pump motor windings are forced air cooled through a NSCCCS heat exchanger which is independent from the intermediate building cooling system.

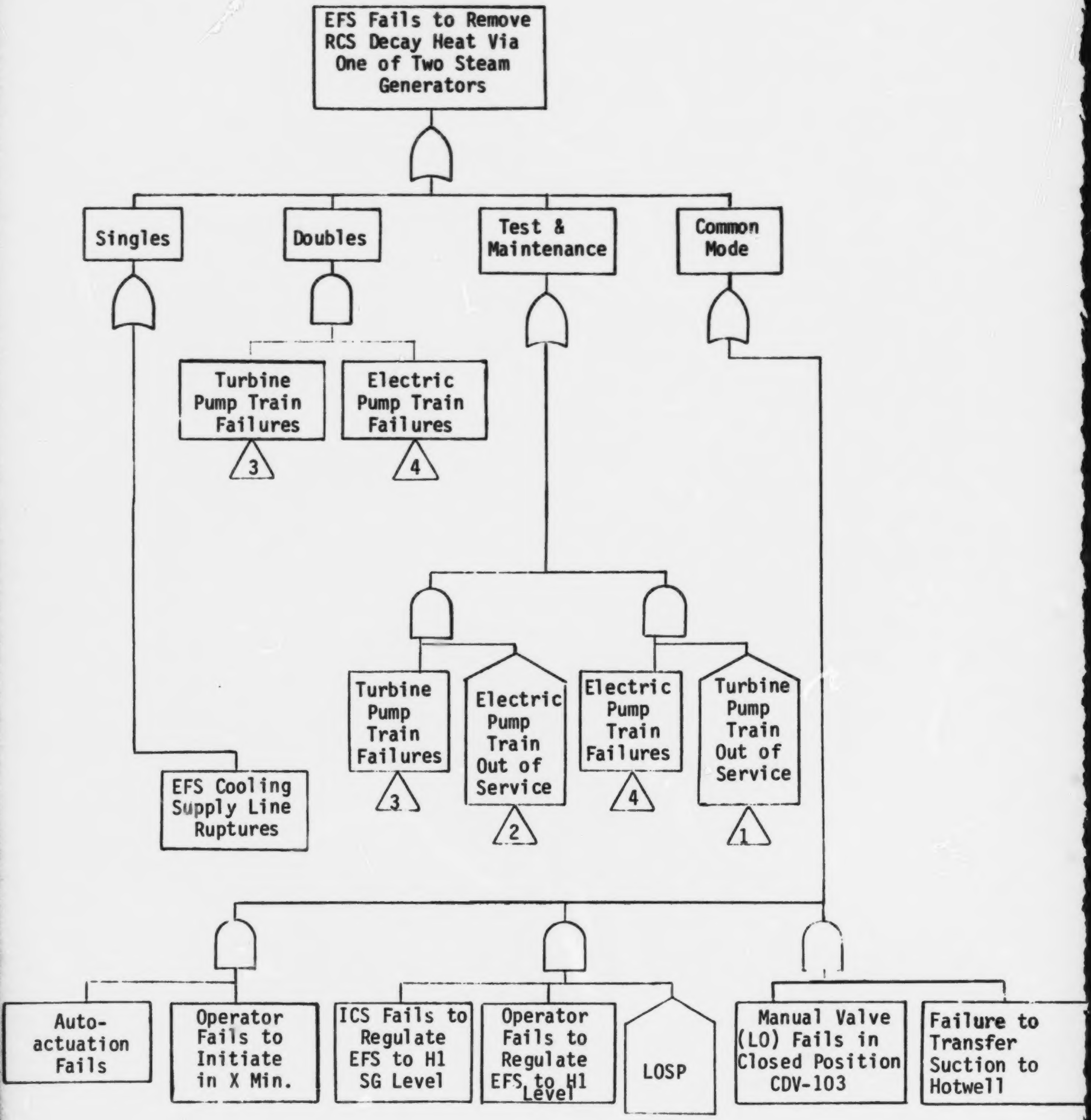

EFS Fails to Remove RCS Decay Heat Via One of Two Steam Generators
Singles
Doubles
Test & Maintenance
Common Mode
Turbine Pump Train Failures
3
Electric Pump Train Failures
4
Turbine Pump Train Failures
3
Electric Pump Train Out of Service
2
Electric Pump Train Failures
4
Turbine Pump Train Out of Service
1
EFS Cooling Supply Line Ruptures
Auto-actuation Fails
Operator Fails to Initiate in X Min.
ICS Fails to Regulate EFS to H1 SG Level
Operator Fails to Regulate EFS to H1 Level
LOSP
Manual Valve (LO) Fails in Closed Position CDV-103
Failure to Transfer Suction to Hotwell

Figure P.7 (1/3) Simplified Fault Tree - Emergency Feedwater System

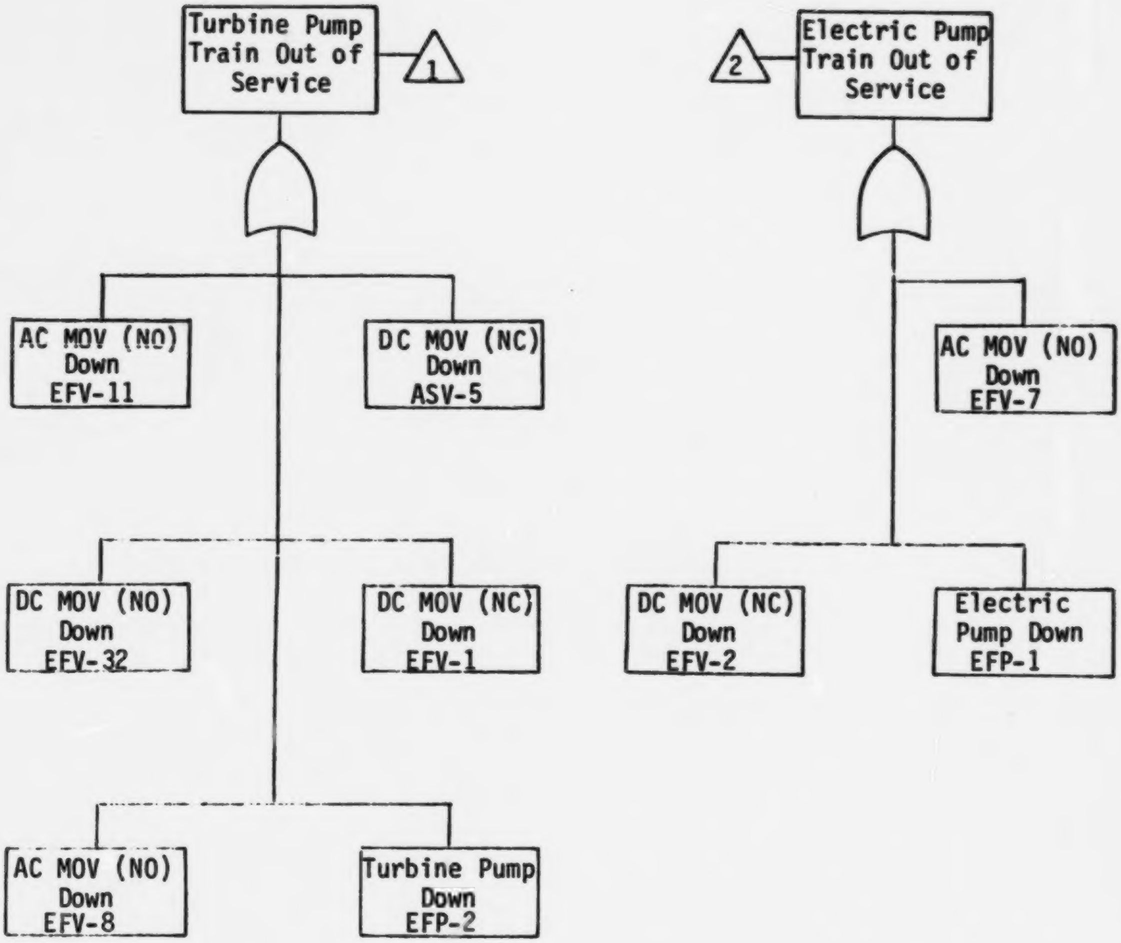

Turbine Pump Train Out of Service
1
Electric Pump Train Out of Service
2
AC MOV (NO) Down EFV-11
DC MOV (NC) Down ASV-5
AC MOV (NO) Down EFV-7
DC MOV (NO) Down EFV-32
DC MOV (NC) Down EFV-1
DC MOV (NC) Down EFV-2
Electric Pump Down EFP-1
AC MOV (NO) Down EFV-8
Turbine Pump Down EFP-2

Figure P.7 (2/3) Simplified Fault Tree - Emergency Feedwater System

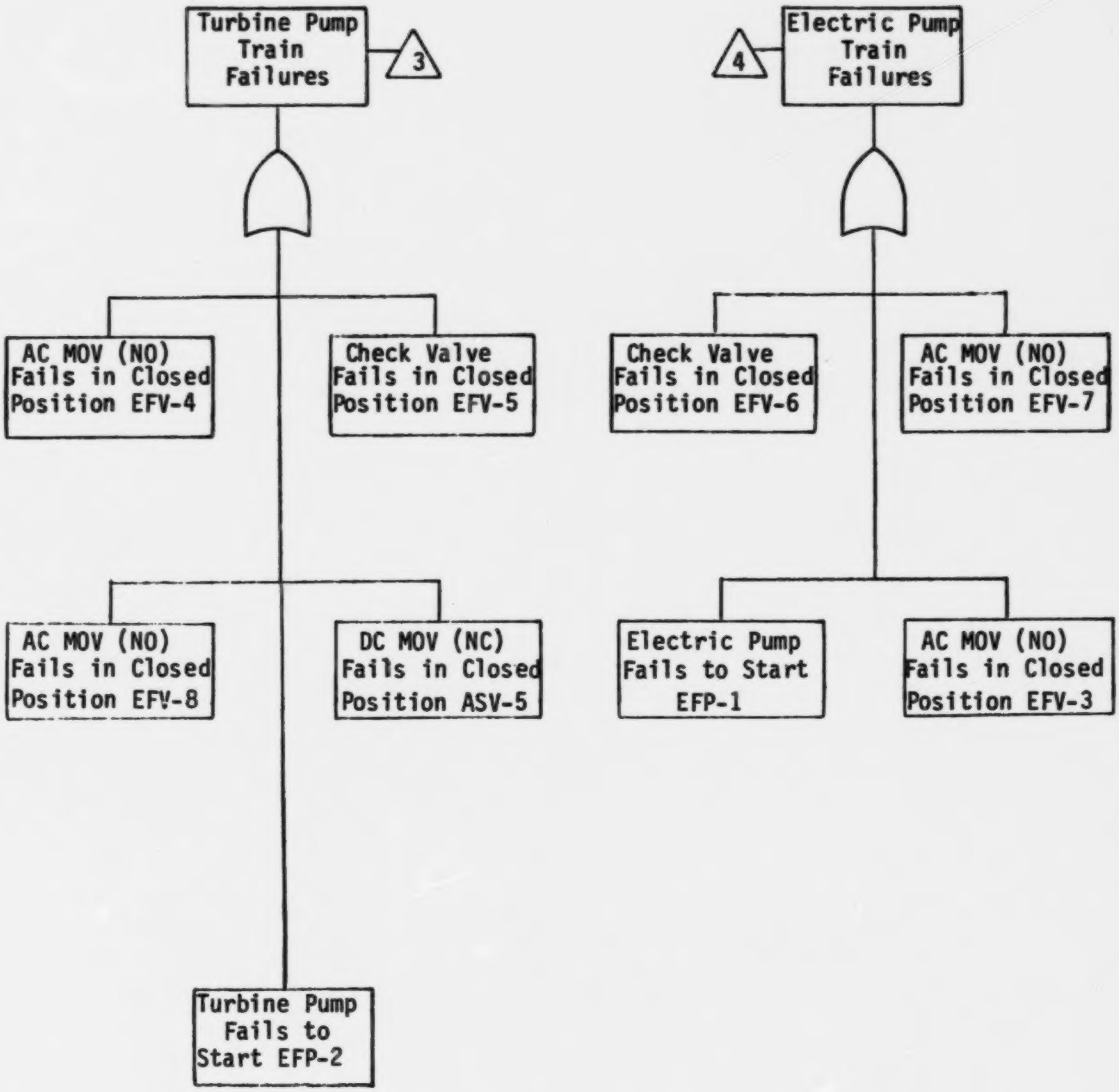

Turbine Pump Train Failures
3
Electric Pump Train Failures
4
AC MOV (NO) Fails in Closed Position EFV-4
Check Valve Fails in Closed Position EFV-5
Check Valve Fails in Closed Position EFV-6
AC MOV (NO) Fails in Closed Position EFV-7
AC MOV (NO) Fails in Closed Position EFV-8
DC MOV (NC) Fails in Closed Position ASV-5
Electric Pump Fails to Start EFP-1
AC MOV (NO) Fails in Closed Position EFV-3
Turbine Pump Fails to Start EFP-2

Figure P.7 (3/3) Simplified Fault Tree - Emergency Feedwater System

P.3 SYSTEM QUANTIFICATION

P.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The Crystal River EFS is basically a two train system with system success defined as successful operation of one of the two trains. Motive power diversity is achieved by employing a turbine-driven pump in Train A and a motor-driven pump in Train B. The turbine-driven pump is self-cooled so system operation is not dependent on AC power. However, DC power is required to open the turbine-driven pump steam admission valve (DC Train B).

For cases where off-site power is available, the unavailability of the EFS was assessed to be principally due to maintenance outages, combinations of hardware failures on both Train A and Train B (double failure), and operator error. Each of these factors is responsible for approximately equal contributions to total system unavailability. For cases where off-site power is lost, the principal contributors to system unavailability are double hardware failures and maintenance outages, which are about an order of magnitude larger than in the non-LOSP case. These contributions are larger here primarily because of the large diesel failure rate, which raises the unavailability of Train B (the motor-driven pump train). Thus, the double failure combinations are dominated by diesel failure and failure of the turbine-driven pump. Turbine-driven pump failure rates were assumed to be about an order-of-magnitude higher than motor-driven pump failure rates - see fault tree quantification tables, and notes for additional details.

P.3.2 SYSTEM FAULT TREE QUANTIFICATION

Two modularized fault trees were constructed for the EFS, one for the case where offsite power is available, and one for the LOSP case.

Table P.1 shows the EFS success requirements with attached notes. Table P.2 contains the top event definitions for the two modularized fault trees. Figures P.8 and P.9 show the two EFS fault trees in terms of the major gates. A point estimate unavailability is shown on these trees for each gate and for the system. Table P.3 shows the Boolean equations that represent the EFS fault trees. Table P.4 shows the quantification of each gate, by component and failure mode for the two fault trees. The attached notes explain the assumptions used in the quantification. Table P.5 summarizes the point estimates for each gate.

Table P.1 EFS - System Success Requirements

INITIATOR	TRAINS	NOTES
$T_2 - T_{2A}$	1/2	1
T_{2A}	1/2	2

NOTES: 1. This group of initiators involves loss of main feedwater by any means other than loss of offsite power. A separate tree is developed for this set of initiators, although the success requirements are the same as for the loss of offsite power case.

2. This initiator is loss of main feedwater due to loss of offsite power. A separate tree is developed for this initiator.

Table P.2 EFS Top Event Definition

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
EF1	Failure of EFS to provide at least 1/2 pump flow to at least 1/2 OTSGs given offsite power is available.	---
EF2	Failure of EFS to provide at least 1/2 pump flow to at least 1/2 OTSGs given offsite power is not available.	---

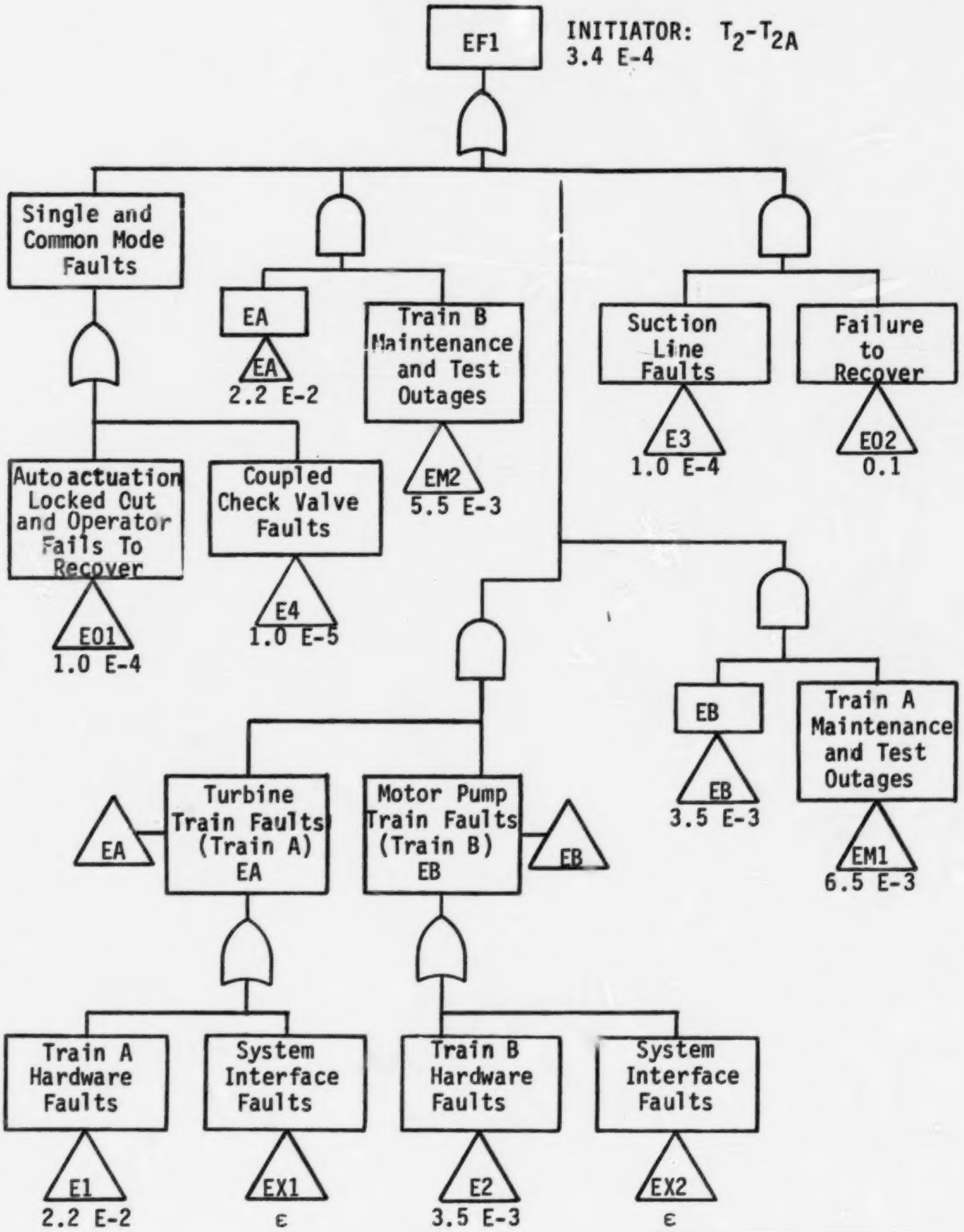
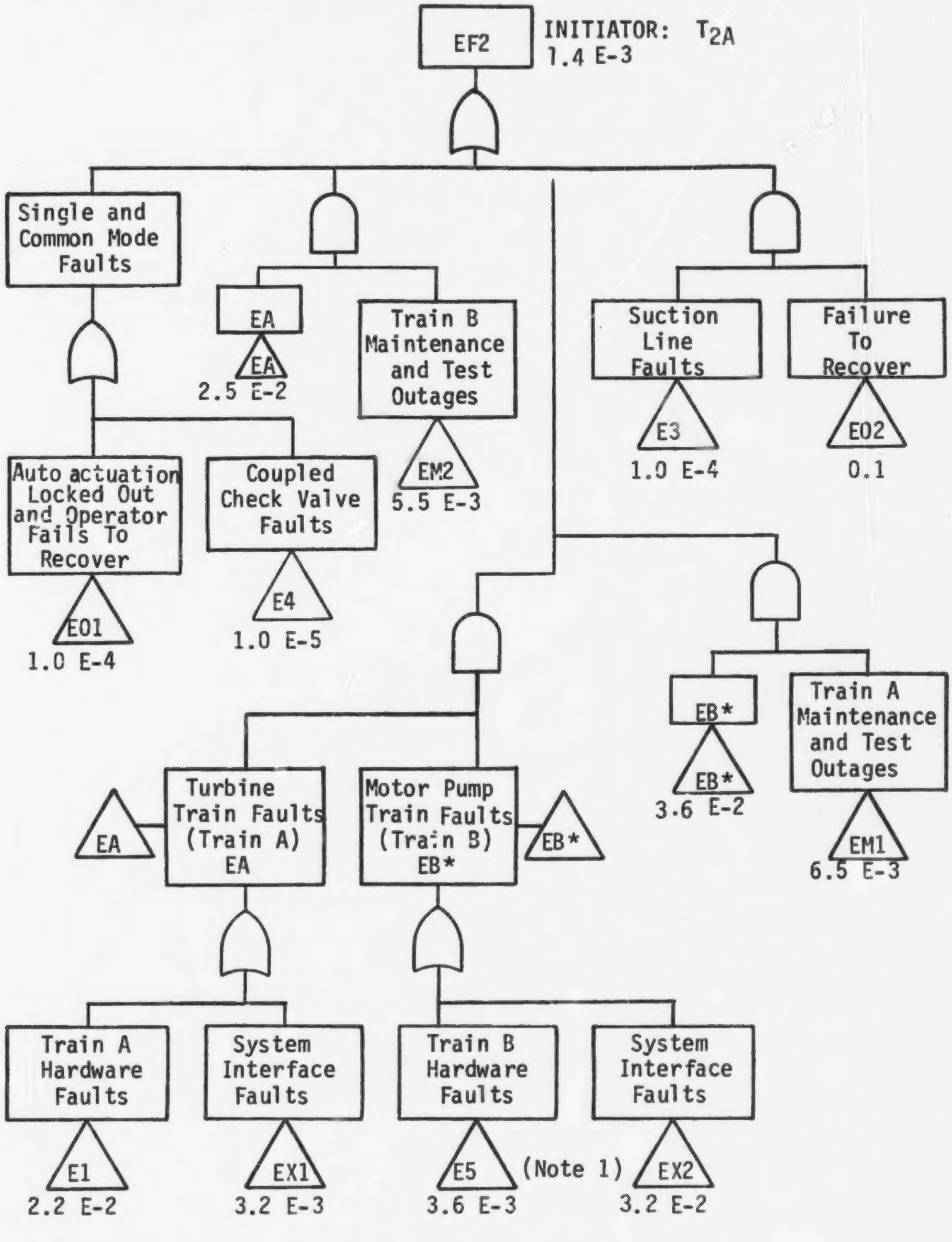

EF1
INITIATOR: T_2-T_{2A}
3.4 E-4
Single and Common Mode Faults
EA
EA
2.2 E-2
Train B Maintenance and Test Outages
EM2
5.5 E-3
Suction Line Faults
E3
1.0 E-4
Failure to Recover
E02
0.1
Auto actuation Locked Out and Operator Fails To Recover
E01
1.0 E-4
Coupled Check Valve Faults
E4
1.0 E-5
EB
EB
3.5 E-3
Train A Maintenance and Test Outages
EM1
6.5 E-3
EA
Turbine Train Faults (Train A) EA
Motor Pump Train Faults (Train B) EB
EB
Train A Hardware Faults
E1
2.2 E-2
System Interface Faults
EX1
ε
Train B Hardware Faults
E2
3.5 E-3
System Interface Faults
EX2
ε

Figure P.8 Modularized Fault Tree for Event "EF1" (Offsite Power Available)


EF2
INITIATOR: T2A
1.4 E-3
Single and Common Mode Faults
EA
EA
2.5 E-2
Train B Maintenance and Test Outages
EM2
5.5 E-3
Suction Line Faults
E3
1.0 E-4
Failure To Recover
E02
0.1
Auto actuation Locked Out and Operator Fails To Recover
E01
1.0 E-4
Coupled Check Valve Faults
E4
1.0 E-5
EB*
EB*
3.6 E-2
Train A Maintenance and Test Outages
EM1
6.5 E-3
EA
Turbine Train Faults (Train A) EA
Motor Pump Train Faults (Train B) EB*
EB*
Train A Hardware Faults
E1
2.2 E-2
System Interface Faults
EX1
3.2 E-3
Train B Hardware Faults
E5
(Note 1)
3.6 E-3
System Interface Faults
EX2
3.2 E-2

Note 1: Gate E 5 differs from Gate E 2 in that it includes operator faults not contained in Gate E 2

Figure P.9 Modularized Fault Tree for Event "EF2" (Offsite Power Not Available)

Table P.3 Emergency Feedwater System

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

$$EF1 = E01 + E4 + EA \cdot EB + EA \cdot EM2 + EB \cdot EM1 + E3 \cdot E02$$

$$EF2 = E01 + E4 + EA \cdot EB^{*} + EA \cdot EM2 + EB^{*} \cdot EM1 + E3 \cdot E02$$

INTERMEDIATE EVENTS

$$EA = E1 + EX1$$

$$EB = E2 + EX2$$

$$EB^{*} = E5 + EX2$$

$$EX1 = DCB$$

$$EX2 = ACA + DCA$$

BEST DOCUMENT AVAILABLE

Table P.4 (1/4) Event "EF1" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
E01		AUTO ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER			1.0 E-4	10^{+}, 10^{-}	0	12
E03	OPERATOR	LOCKS OUT AUTO ACTUATION	D		1.0 E-3	10^{+}, 10^{-}	0	
E04	OPERATOR	FAILS TO RECOVER	D		0.1	10^{+}, 10^{-}	0	
					Π=1.0 E-4			
E4		COUPLED CHECKVALVE FAULTS (FWV-43, 44)	(1.0 E-4)(0.1)		1.0 E-5	2^{+}, 2^{-}	B	
EA		TURBINE TRAIN FAULTS (TRAIN A)						
E1		TRAIN A HARDWARE FAULTS			2.2 E-2	3^{+}, 3^{-}	S	
	MOV EFV-4	INADVERTENTLY CLOSED	D		3.0 E-6	10^{+}, 10^{-}		1
	MOV EFV-4	PLUGGED	D		1.0 E-4	3^{+}, 3^{-}		
	MOV EFV-8	INADVERTENTLY CLOSED	D		3.0 E-4	10^{+}, 10^{-}		2
	MOV EFV-8	PLUGGED	D		1.0 E-4	3^{+}, 3^{-}		
	EFV-5	CHECKVALVE FAILS TO OPEN	D		1.0 E-4	3^{+}, 3^{-}		
	ASV-5	FAILS CLOSED	D		1.0 E-3			
	ASV-5	AUTO ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER	D		1.0 E-4	3^{+}, 10^{-}		3, 12
	CTRL. CIRCUIT	FAILS TO TRANSFER (RELAY FAILS TO ENERGIZE)	D		1.0 E-4	3^{+}, 3^{-}		
	EFP-2	TURBINE PUMP FAILS TO START	D		2.0 E-2	3^{+}, 3^{-}	S	4
	EFP-2	TURBINE PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5/HR	24	7.2 E-4	10^{+}, 10^{-}		5
					Σ=2.2 E-2			
EX1		SYSTEM INTERFACE FAULTS (NON LOSP)			ϵ			
DCB	DC ESB	DC POWER TRAIN B FAILS						
		NON LOSP			ϵ			
EB		MOTOR PUMP TRAIN FAULTS (TRAIN B)						
E2		TRAIN B HARDWARE FAULTS			3.5 E-3	2.4^{+},1.5^{-}	0	
	MOV EFV-3	INADVERTENTLY CLOSED	D		3.0 E-6	10^{+}, 10^{-}	0	1
	MOV EFV-3	PLUGGED	D		1.0 E-4	3^{+}, 3^{-}		
	MOV EFV-7	INADVERTENTLY CLOSED	D		3.0 E-4	10^{+}, 10^{-}	0	2
	MOV EFV-7	PLUGGED	D		1.0 E-4	3^{+}, 3^{-}		
	EFV-6	CHECK VALVE FAILS TO OPEN	D		1.0 E-4	3^{+}, 3^{-}		
	EFP-1	MOTOR PUMP FAILS TO START	D		1.0 E-3	3^{+}, 3^{-}		
	EFP-1	MOTOR PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5	24	7.2 E-4	10^{+}, 10^{-}		
	CTRL. CIRCUIT	FAILS TO ACTUATE (RELAY)	D		1.0 E-4	3^{+}, 3^{-}		
	EFP-1 BRK.	FAILS TO TRANSFER	D		1.0 E-3	3^{+}, 3^{-}		
	AUTO. ACT.	AUTO-ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER	D		1.0 E-4	3^{+}, 10^{-}	0	6, 12
					Σ=3.5 E-3			

Table P.4 (2/4) Event "EF1" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
EX2		SYSTEM INTERFACE FAULTS (NON LOSP)			ϵ			
DCA	DC E5A	DC POWER TRAIN A FAILS						
		NON LOSP			ϵ			
ACA		AC TRAIN A FAILS						
		NON LOSP			ϵ			
		LOSP			3.2 E-2			
EM1		TRAIN A MAINTENANCE AND TEST OUTAGES			6.5 E-3	3^+, 3^-	M	7, 8
	MOV EFV-11	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	MOV EFV-32	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	MOV ASV-5	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	EFP-2	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	3^+, 3^-	M	8
					Σ=6.5 E-3			
EM2		TRAIN B MAINTENANCE AND TEST OUTAGES			5.5 E-3	3^+, 3^-	M	7, 8
	MOV EFV-14	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	MOV EFV-33	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	MOV EFV-7	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3^+, 3^-	M	10
	EFP-1	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	3^+, 3^-	M	8
					Σ=5.5 E-3			
		SUCTION LINE FAULTS			1.0 E-5	2^+, 2^-	0	
E3	CDV-103	VALVE PLUGGED	D		1.0 E-4	3^+, 3^-		
E02	OPERATOR	FAILS TO RECOVER	D		0.1	2^+, 2^-	0	9
					π=1.0 E-5			

BEST DOCUMENT AVAILABLE

Table P.4 (2/4) Event "EFI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
EX2		SYSTEM INTERFACE FAULTS (NON LOSP)			ε			
DCA	DC E5A	DC POWER TRAIN A FAILS						
		NON LOSP			ε			
ACA		AC TRAIN A FAILS						
		NON LOSP			ε			
		LOSP			3.2 E-2			
EM1		TRAIN A MAINTENANCE AND TEST OUTAGES			6.5 E-3	$3^+, 3^-$	M	7, 8
	MOV EFV-11	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-32	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV ASV-5	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	EFP-2	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	$3^+, 3^-$	M	8
					Σ=6.5 E-3			
EM2		TRAIN B MAINTENANCE AND TEST OUTAGES			5.5 E-3	$3^+, 3^-$	M	7, 8
	MOV EFV-14	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-33	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-7	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	EFP-1	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	$3^+, 3^-$	M	8
					Σ=5.5 E-3			
		SUCTION LINE FAULTS			1.0 E-5	$2^+, 2^-$	0	
E3	CDV-103	VALVE PLUGGED	D		1.0 E-4	$3^+, 3^-$		
E02	OPERATOR	FAILS TO RECOVER	D		0.1	$2^+, 2^-$	0	9
					π=1.0 E-5			

BEST DOCUMENT AVAILABLE

Table P.4 (4/4) Event "EF2" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
EX2		SYSTEM INTERFACE FAULTS (LOSP)			3.2 E-3			
DCA	DC E5A	DC POWER TRAIN A FAILS						
		LOSP			3.2 E-3			
ACA	AC TRAIN A	AC TRAIN A FAILS						
		NON LOSP			ε			
		LOSP			3.2 E-2			
EM1		TRAIN A MAINTENANCE AND TEST OUTAGES			6.5 E-3	$3^+, 3^-$	M	7, 8
	MOV EFV-11	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-32	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV ASV-5	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	EFP-2	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	$3^+, 3^-$	M	8
					Σ=6.5 E-3			
EM2		TRAIN B MAINTENANCE AND TEST OUTAGES			5.5 E-3	$3^+, 3^-$	M	7, 8
	MOV EFV-14	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-33	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	$3^+, 3^-$	M	10
	EFP-1	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	$3^+, 3^-$	M	8
					Σ=5.5 E-3			
E3·E02		SUCTION LINE FAULTS			1.0 E-5	$2^+, 2^-$	0	
E3	CDV-103	VALVE PLUGGED	D		1.0 E-4	$3^+, 3^-$		
E02	OPERATOR	FAILS TO RECOVER	D		0.1	$2^+, 2^-$	0	9
					π=1.0 E-5			

BEST DOCUMENT AVAILABLE

Table P.4 Emergency Feedwater System

QUANTIFICATION TABLES

NOTES

1 This fault was assessed as an inadvertent act of commission (1.0 E-3/year) since the valve is not closed by any procedure. The valve is checked once per shift. Therefore, the fault exposure time is 8 hours. The fault is therefore assessed as (1.0 E-3)(8/8760)=1.0 E-6.

2 This valve is closed on monthly test. The basic act of leaving the valve closed was assessed as 1.0 E-2/month. The valve is checked every 8 hours; so the fault duration time is 8 hours. Therefore, the fault was assessed as (1.0 E-2)(8/720)=1.1 E-4.

3 The basic fault of leaving auto actuation of steam admission valve ASV-5 locked out was assessed as 1E-3. An additional probability of the operator failing to recover of 0.1 was assumed. The total fault was assessed as 1.E-4. The fault probability could be lower because the auto actuation is verified to be in AUTO once every shift.

4 The demand probability for the turbine fails to start was obtained from NUREG/CR-1205 (Reference P-1) which contains a summary of B&W turbine pump failure rates.

5 The turbine pump failure rate was obtained from Appendix III of WASH-1400 since Reference P-1 did not contain data for turbine failure to run.

6 This is a similar fault to that described in Note 3, except that the electric-driven pump auto actuation is locked out.

7 Test outages were assessed to not contribute to system unavailability since valves EFV-3,4,7, and 8 open automatically on receipt of an actuation signal.

8 Maintenance outages were assessed by assuming one train outage every 2 months. This outage was converted to a component outage frequency of 0.1/month. Average maintenance outage times of 7 hours for valves and 19 hours for pumps were assumed.

9 The operator could recover here by transferring suction from the condensate storage tank to the hotwell. DC valves EFV-1 and EFV-2 would have to open to supply their respective train.

10 It was assumed that valve maintenance would require isolation of the valve being maintained by closing valves on either side of the maintained valve.

Table P.4 Emergency Feedwater System (con't)

QUANTIFICATION TABLES

NOTES

11 Operator is required to load motor pump EFP-1 on to AC bus (Train A) after D.G. A starts, this fault was assessed as 1.E-3 with 10% chance that he would recover.

12 Auto-actuation faults in E1 and E2 and the fault E01 are separate events. The former two are associated with individual trains, while the latter refers to the entire system. The fault probabilities indicated are probably very conservative since auto-actuation is verified once each shift and is monitored in the control room.

References

P-1 "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978," prepared by W. H. Sullivan and J. P. Poloski, EG&E Idaho, Inc., for the U.S. Nuclear Regulatory Commission, (EG&E Report No. EGG-EA-5044) NUREG/CR-1205, January 1980.

Table P.5 EFS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
E01	1.0 E-4
E03	1.0 E-3
E04	0.1
E4	1.0 E-5
E1	2.2 E-2
DCB	ε* 3.2 E-3**
E2	3.5 E-3
DCA	ε* 3.2 E-3**
ACA	ε* 3.2 E-2**
EM1	6.5 E-3
EM2	5.5 E-3
E3	1.0 E-4
E02	0.1
E5	3.6 E-3

*Offsite power available

**Offsite power not available

Distribution:

USNRC Distribution Contractor (CDSI) (155)
7300 Pearl Street
Bethesda, Maryland 20014
130 Copies for AN
25 Copies for NTIS

Author selected distribution - 25 Copies
(List available from author.)

4400	A. W. Snyder
4410	D. J. McCloskey
4412	J. W. Hickman (3)
4412	D. D. Carlson
4412	W. R. Cramond
4412	D. D. Drayer
4412	F. T. Harper
4412	S. W. Hatch
4412	A. M. Kolaczkowski
4412	G. J. Kolb
4412	A. C. Payne
4412	R. G. Spulak
4412	T. A. Wheeler
4413	N. R. Ortiz
4414	G. B. Varnado
4415	D. J. McCloskey, Actg.
4416	L. D. Chapman
3141	L. J. Erickson (5)
3151	W. L. Garner (3)
8214	M. A. Pound

[illegible] 493